Human Capital Agenda Security 2023 – 2026

HSD
securitydelta.nl

Centrum voor
Veiligheid en
Digitalisering

Human Capital Agenda Security 2023 – 2026

Management samenvatting

De afgelopen 4 jaar zijn van invloed geweest op veiligheidstalenten op manieren die niet waren voorzien in de vorige Human Capital Agenda Security. Bedreigingen zoals de COVID-pandemie en de oorlog in Oekraïne en andere geopolitieke spanningen, vooruitgang in de toepassing van kunstmatige intelligentie en wet- en regelgeving voor cyberbeveiliging en een oververhitte arbeidsmarkt in Nederland hadden allemaal invloed op het werken aan veiligheid. De belangrijkste uitdaging blijft echter hetzelfde: voldoende talent om gelijke tred te houden met veranderende bedreigingen en economische kansen, waardoor het aantal moeilijk vervulbare vacatures afneemt. Dit kan worden bereikt met meer mensen, wat mogelijk leidt tot concurrentie met andere banen, maar bij voorkeur door efficiënter en beter werken, taakverdeling, coördinatie en samenwerking. Dit vereist collectieve actie.

We verwachten dat de digitalisering van de samenleving zich zal verbreden en verdiepen. Elke sector heeft ermee te maken, ook indirect door de waardeketens waar ze deel van uitmaken, en het heeft invloed op steeds meer processen. Met de toenemende afhankelijkheid van onze digitale infrastructuur is het gebrek aan talent zélf een belangrijk veiligheidsrisico geworden. Om te groeien in een krappe arbeidsmarkt zijn werkgevers op zoek naar productiviteit door middel van automatisering en een efficiëntere organisatie. Ze gaan op zoek naar risicoverlaging in de toeleveringsketen en door samenwerking. Tenzij onze risicobereidheid snel verandert, wat we niet verwachten, zal de behoefte aan talent op het gebied van beveiliging groot blijven.

Deze doorrollende agenda is een gedeelde ambitie en basis voor verdere samenwerking op lokaal, regionaal en nationaal niveau. We zijn blij met de steun van al 70 organisaties. Met de scope op veiligheid in een digitaliserende samenleving wordt een analyse gepresenteerd die resulteert in belangrijke bevindingen vanuit vijf perspectieven: Talent, Werk, Onderwijs, Veiligheid en Maatschappij. Enkele grotere knelpunten die zijn geïdentificeerd, zijn Talententekort, Onaantrekkelijk werkveld, Onaantrekkelijke banen, Geen carrièreperspectief, Beperkte investeringen en Gebrek aan begrip. De belangrijkste bevindingen en knelpunten vormen de basis voor 25 interventies gericht op de arbeidsmarkt van digitale veiligheid. Deze omvatten het versterken en monitoren van arbeidsmarktinzichten, de ontwikkeling van specifieke trainingsmodules en -programma's voor professionals en carrièreswitchers, flexibilisering van de werkverdeling, het aantrekken van ondervertegenwoordigde groepen en het promoten van werk in de beveiliging, ondersteuning van HR en effectieve leergemeenschappen en competentieontwikkeling op het gebied van beveiliging.

Samenhang, coördinatie en uitvoering zijn op dit moment meer incidenteel en meestal niet gefinancierd, deze agenda is een stap vooruit in dit opzicht en moet worden geborgd. Lokale, regionale en sectorale vertalingen moeten gemaakt worden en investering is nodig om de genoemde ambities te ondersteunen en te realiseren. Een gezamenlijk financieel- en actieplan op basis van deze agenda door de partners en ondersteuners is de volgende stap.

Human capital bottlenecks

Themes and actions for human capital in security

Management Summary

The last 4 years impacted security talent in ways not foreseen in the previous Human Capital Agenda Security. Threats such as the COVID pandemic and the war in Ukraine and other geopolitical tensions, advancements in Artificial Intelligence application and regulatory cybersecurity frameworks, an overheated labour market in The Netherlands all impacted working on security. The main challenge remains the same: enough talent to keep pace with evolving threats and economic opportunities, reducing the number of hard to fill job openings. This can be accomplished with more people, possibly leading to competition with other jobs, but preferably by more efficient and skilled working, division of labour, coordination, and collaboration. This requires collective action.

We expect the digitisation of society to widen and deepen. Every sector is affected by it, also indirectly by the value chains they are part of, and it impacts more and more processes. With the growing dependencies on our digital infrastructure the lack of talent itself has become a main security risk. To grow in a tight labour market, employers are looking for productivity through automation and more efficient organisation. They are starting to look for reducing risk in the supply chain and through cooperation. Unless our risk appetite changes quickly, what we don't expect, the need for talent working on security will remain high.

This rolling agenda is a shared ambition and basis for further collaboration on local, regional, and national level. We are delighted with the support of 70 organisations already. With its scope on security in a digitising society, an analysis resulting in key findings from five perspectives is presented: Talent, Work, Education, Security and Society. Several bigger bottlenecks identified are Talent shortage, Unattractive field, Unattractive jobs, No career perspective, Limited investment, and a Lack of understanding. The key findings and main bottlenecks are the basis for 25 interventions aimed at the labour market of digital security. These include the strengthening and monitoring of labour market insights, development of specific training modules and -programs for professionals and career switchers, flexibilization of the division of work, attracting underrepresented groups and promoting work in security, support for HR and effective learning communities and security competence development.

Coherence, coordination, and execution are currently more incidental and mostly unfunded, this agenda is a step up in this respect and needs to be secured. Local, regional, and sectoral translations need to be made and invested in to support and realise the mentioned ambitions. A joint financial and action plan based on this agenda by the partners and supporters is the next step.

Human capital bottlenecks

Table of contents

1. Introduction

The last 4 years impacted security talent in ways not foreseen in the previous Human Capital Agenda Security (HCA Security 2019 – 2022[1]). Security threats such as the COVID pandemic and the war in Ukraine and other geopolitical tensions, advancements in Artificial Intelligence application and regulatory cybersecurity frameworks, an overheated labour market in The Netherlands all impacted working on security. Digitisation and security awareness grew this way, resulting in both opportunities and threats for security work. The main challenge remains the same: enough talent to keep pace with evolving threats and economic opportunities. This can be accomplished with more people, possibly leading to competition with other jobs, but preferably by more efficient and skilled working, division of labour, coordination, and collaboration. This requires collective action.

Something that changed in the last years is the perception of Human Capital in security and responsibility for security. With the tight labour market there is an additional strain on human resources while the demand for security remains high. Digitisation and automation grow, to see and do more with less people. But this requires digitally skilled talents working on security in a broader sense and expands the digital attack surface, security in a narrower sense. At the same time, safe working in the digitising society is no longer only an IT-matter. For instance in cybersecurity, people are often considered 'the weakest link'. But even if this would be the case: stating it doesn't solve the problem, growing competencies and talents for both specialists and other workers does. With the growing dependencies on our digital infrastructure the lack of talent itself has become a main security risk[2].

We expect the digitisation of society to widen and deepen. Every sector is affected by it, also indirectly by the value chains they are part of, and it impacts more and more processes. To grow in a tight labour market, employers are looking for productivity through automation and more efficient organisation. They are starting to look for reducing risk in the supply chain and through cooperation. Unless our risk appetite changes quickly, what we don't expect, the need for talent working on security will remain high. For these reasons, and the shared need from our partners, we developed this Human Capital Agenda Security 2023-2026. 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 digitisation and is resilient to advanced physical and digital threats. There is enough 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 organisations. Security tasks and competencies are part of everybody's job. Working on security offers talent a sustainable career perspective and is inclusive and diverse to meet all challenges. It 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 Security Delta (HSD). In 2022 the Centre for Safety and Digitisation (CVD) started in the east of The Netherlands with similar ambitions regarding talent for security. The relation between ICT and the security field is evident, cluster and network organisations Topsector ICT Netherlands, ECP, dcypher and branch organisations such as CVNL have advocated IT- and digital security related skills development and the Action Plan Green and Digital Job[3], Human Capital Agenda ICT[4], Plan of Attack Chronic Shortage IT-talent[5] and CA-ICT[6] (Education Fund for ICT labour market) as well. The Cyber Security Council study and National Cybersecurity Strategy state the need for more cybersecuritytalent. Therefore, the Ministry of Education, the Ministry of the Interior, the Ministry of Economic Affairs (including DTC and dcypher) and the Ministry of Justice and Security (including the NCTV and the NCSC) all support the attraction and development of more talent in cybersecurity. This agenda will lay the groundwork for future cooperation with the Ministry of Economic Affairs and the National Government, as well as Topsector ICT and the public-private collaboration platform dcypher, aimed at alignment with national policies and ambitions to maximize execution power, coherence and impact.

Together, we can realise results that apart we cannot.

Therefore, this agenda is a shared ambition and basis for further collaboration on local, regional, and national level. We are delighted with the support already shown by many organisations (*see Appendix 1 – Consulted organisations*) through their engagement or leadership in one or more of the activities in this agenda, or their support for the agenda as a whole. We look forward to realising the ambitions with them and others to join in our combined efforts.

The chosen approach and actions in the previous agenda have proven fruitful as substantiated by the results shared in Appendix 2 – Results HCA Security 2019 – 2022. Despite efforts to close the cybersecurity workforce gap, the (ISC)[2] Cybersecurity workforce study 2022, shows that although the cyber workforce in EMEA grew with almost 12%, the gap has grown more than twice as much. The competition for attracting talent is fierce. The longer-term ambition is to reduce the number of hard to fill job openings (those that are open for more than 45 days), thereby making The Netherlands more secure and grow the economic impact of a thriving sector. This agenda builds on previous agendas and programmes of partners by using their successful actions, with the following principles:

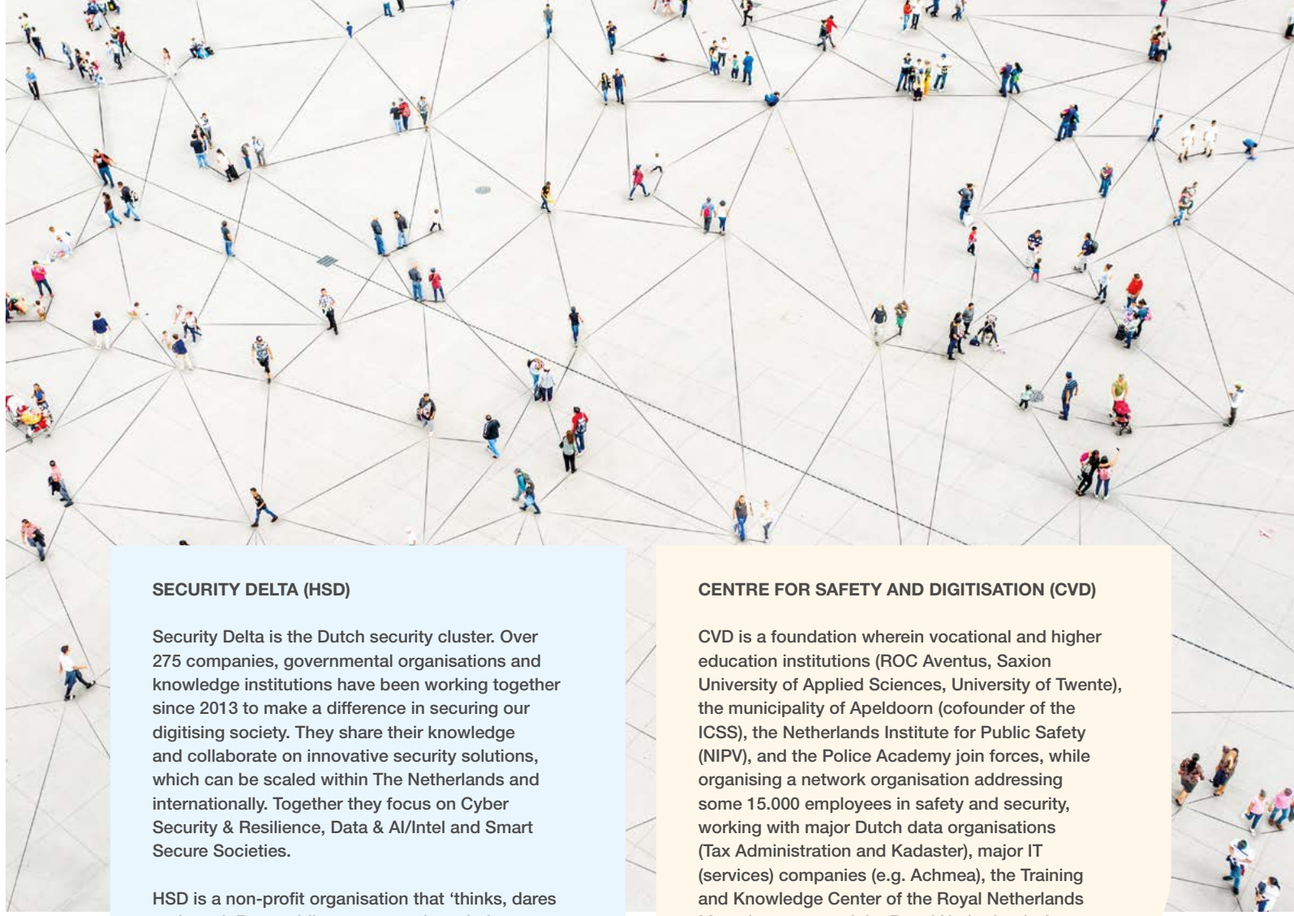
- **Focussing the scope to security in a digitising society.** The previous agendas had a wide scope on security or highlighted just one specific part or angle. Each for a good reason. While broad and deep is still necessary for market analysis, broader talent development, career tracks and security as a whole, most of the changes take place where new opportunities and threats appear, often accompanied or caused by digitisation. This will be our primary focus and area of intervention. It is broader than cybersecurity, but narrower than security. Algorithms and AI development, both within security and cybersecurity, are in scope for instance but 'traditional' security tasks like patrolling in the physical domain without digital elements are out of scope.

- **To attack Human Capital challenges, you need actions from different perspectives.** Where we used to focus on *talents* and *employers* mainly or *education* only, we need to include perspectives and developments from the *security* field and *society* itself. Changes in security threats, technology, and broader labour market, impact the human capital needs and interventions. The broadening of perspectives needs to be accompanied by refining our view, from job profiles to competence and task level. By doing so, the five perspectives can find a common denominator.

- **The area of application is national, hence the collaboration with partners acting nationally.** It does need translation to regional and local level as well, to optimally fit and combine with actions taken at those levels. Therefore, we scale up the coordination and collaboration with those stakeholders. For some interventions, a sectoral approach is more productive and underway. We are already connected with several sectors to support their Human Capital ambitions in the security work domain. Coordination and collaboration nationwide also make it possible to investigate the dependencies and interactions between roles to limit the unproductive fighting over personnel resources.

In this Human Capital Agenda Security, we first take a closer look at the security labour market in the Netherlands. To gain better insights we describe and analyse the labour market along the developments in five connected perspectives that are relevant for human capital in security: Talent, Education, Work, Security and Society. The results of this analysis lead to the identification of six underlying bottlenecks and eight talent groups. Relevant actions and interventions are gathered and structured, both existing and intended initiatives from our partners and other parties in the security cluster, to overcome the bottlenecks for the specified talent groups in this agenda.

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 our combined networks' expertise, execution power and ambitions. Detailing the follow-up, naming the leaders and supporters of actions, and organising execution if this is not yet in place, is the next step.



SECURITY DELTA (HSD)

Security Delta is the Dutch security cluster. Over 275 companies, governmental organisations and knowledge institutions have been working together since 2013 to make a difference in securing our digitising society. They share their knowledge and collaborate on innovative security solutions, which can be scaled within The Netherlands and internationally. Together they focus on Cyber Security & Resilience, Data & AI/Intel and Smart Secure Societies.

HSD is a non-profit organisation that 'thinks, dares and acts'. By providing access to knowledge, innovation, market, finance, and talent, HSD takes care of the preconditions for a successful security cluster. We do this with the common goal of strengthening the Dutch economy, increase employment rates and making The Netherlands more secure.

CENTRE FOR SAFETY AND DIGITISATION (CVD)

CVD is a foundation wherein vocational and higher education institutions (ROC Aventus, Saxion University of Applied Sciences, University of Twente), the municipality of Apeldoorn (cofounder of the ICSS), the Netherlands Institute for Public Safety (NIPV), and the Police Academy join forces, while organising a network organisation addressing some 15.000 employees in safety and security, working with major Dutch data organisations (Tax Administration and Kadaster), major IT (services) companies (e.g. Achmea), the Training and Knowledge Center of the Royal Netherlands Marechaussee, and the Royal Netherlands Army.

[1] https://securitydelta.nl/media/com_hsd/report/231/document/HSD-Human-Capital-Agenda-Security-Webversie.pdf
[2] The Netherlands Cybersecurity Strategy 2022-2028 https://english.ncsc.nl/publications/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028
[3] https://www.rijksoverheid.nl/documenten/kamerstukken/2023/02/03/inzet-op-arbeidsmarktkrapte-in-de-klimaat-en-digitale-transitie-het-actieplan-groene-en-digitale-banen
[4] The ICT Human Capital Agenda (HCA ICT) is the leading agenda of the Ministry of Economic Affairs and Climate Policy to work towards: A sufficient number of well-trained ICT professionals for the successful digital transformation of The Netherlands. Platform Talent for Technology (The Dutch National STEM Platform) is in the lead and executes all activities in close collaboration with regional and national organisations.
[5] https://www.nldigital.nl/wp-content/uploads/2023/02/Aanvalsplan-Chronisch-Tekort-ICTers.pdf

2. Security labour market in the Netherlands

To better understand the shortage of talent in the security labour market, it is important to know the market and therefore define the scope of the security labour market, human capital and education. In this agenda we approach the security labour market in the Netherlands along the lines of five connected perspectives or themes that are relevant for human capital in security: talent, education, work, the security field and societal developments. Relevant developments from each of these themes will be highlighted in this chapter.

2.1 Scope

What type of work belongs to the security domain, what do we mean by human capital and what type of education is in scope? Security related work entails a broad scope of activities, tasks and roles[7]. We define **security workers** in a broad sense:

- the traditional security-workers, including: police officers, firefighters, military personnel and security guards;
- the non-traditional security workers contributing to 'security' at a more institutional level: risk managers, lawyers, judges, privacy officers, compliance officers, fraud examiners, etc.;
- IT occupations directly impacting security, including experts in cybersecurity, AI, Blockchain, encryption and quantum computing; and
- other people working on security tasks as an addition to their regular work.

As mentioned in Chapter 1, our focus is on security related tasks in the context of a digitising society. This is part of all mentioned types of security workers but does not include them all. We do see a development in making more use of digital technology by all types.

In recruiting talent and developing security professionals, different sectors fish in the same pond. Not only the safety & security sector needs cybersecurity specialists for instance, but they are also in high demand in telecom, financial services, healthcare and other sectors. So, we define the **security labour market** as those working on security, independent of the sector they work in and their security role (*see Figure 1*). We focus on shifting fields of work and have a forward outlook, the 'traditional' security-workers such as security guards is not our focus area. Most of the changes take place where new opportunities and threats appear, often accompanied or caused by digitisation. However, where demands overlap with more traditional functions, we embrace cooperation and joint efforts.

By **human capital** we mean the competences, knowledge, skills, and personality traits that enable people to create value. This agenda has a national scope to enhance human capital for innovative and digital security.

The level of education and training is mostly from medium until higher level of abstraction (strongly tied to current market demand), both formal education and non-formal training and certification in the security domain. Primary and secondary education is part of our scope when it connects strongly with our primary objectives, raising awareness, basic security skills and interest in further education in this field.

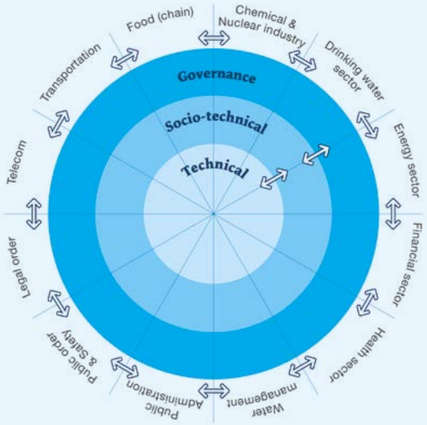


Figure 1: Conceptualisation of Cyberspace[8] in three layers (rings) and sub-domains (pie points)

[7] CBS (2018). Education and labour market in the security domain

[8] 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.

In this agenda we approach the security labour market in The Netherlands along the lines of five connected perspectives or themes that are relevant for human capital in security: talent, education, work, the security field and societal developments (*see Figure 2*). The rest of this chapter will highlight relevant developments from each of these themes.

2.2 Talent

The availability of adequately trained people is crucial for a well-functioning security labour market. Staff shortages now play out in all sectors, including the safety & security domain.

People working in security occupations and security-related functions are more often highly educated[9]. They often fall in the middle age range, which calls for attracting young talent and monitoring the overall age structure of the workforce.

In this section we outline talent from three perspectives: individual talent, competences, and talent groups.

Figure 2: Themes in the Human Capital Agenda Security 2023-2026

2.2.1 Talent from an individual's perspective

Generally, regardless the work status of an individual (student, employed, self-employed, job seeker), the choice for a certain job, function, or role is made based on several factors, such as:

- personal interest, capabilities and ambitions;
- influences of parents, family, friends and peers;
- personal basic/professional education and position on the labour market;
- subjective career expectations and objective growth perspectives in sectors, occupations, organisations;
- availability of personal guidance, such as job and career coaches, personal development programmes;
- values and beliefs of the generation to which an individual belongs; and
- any other relevant factors.

Growing the number of people choosing for a career in for instance cybersecurity can use these factors to influence the outcomes of this decision-making process. 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, personal leadership, problem solving skills and the ability to cope with stress[10] are examples of traits that they all need.

Another talent group that can be grown for digital security demand are internationals[11], although the demand for these is not only high in The Netherlands[12]. Attracting international talent for digital security work requires many actions, from positioning the location, housing to employer readiness. Organisations that employ people from different generations[13] need to address the challenge that younger generations in general have other values and beliefs compared to the older generations.

Needs of Generation Z and required leadership

Generation Z, or Gen Z, have a different set of priorities when it comes to the world of work than their previous generations. For the security field this is specifically important because of the earlier mentioned higher average age and need for digital skills that are more present under younger groups[14]. Commitment from business leaders is needed to engage this new generation of workers, while still accommodating the established members of the workforce. According to the World Economic Forum, an empathetic leadership style is required to attract and retain the future workforce, incorporating five key elements[15]:

- foster creativity and a start-up culture (employee entrepreneurship);
- organise flexibility (working hours, hybrid working, remote working);
- encourage diversity (diversity-equity-inclusion in teams, representative leadership);
- commit to globally guided values (sense of purpose, eco-anxiety); and
- train in future skills (also those without college degrees).

In addition, growth- and development opportunities embedded in a setting of lifelong learning are also key. Obviously, not only Gen Z, but also older generations would benefit from such new leadership style.

What does this mean for the security labour market?

Employers in security may need to change their labour market policy, identify the specific wishes and expectations of young security talent, find out how they can be reached for work within the security sector or security-related work in other sectors. Employers may also search new target groups in international communities or channels, untapped potential in terms of diversity of the workforce. We do hear some reluctance to employ international talent for security jobs, both because of risk and importance of culture including language in security work. For software developers the English language may suffice, for working on security that is not always the case. Welcoming specific nationalities and for specific tasks in combination with training to make the cultural fit, grows the talent pool.

Once onboarded as new hires, employers will have to take special actions to retain security talent[16], for instance: offer flexible working hours, learning and development opportunities, choice between different career paths, mentoring and/or personal coaching, a stimulating work climate and a modern leadership style.

2.2.2 Competences

A relatively new angle to recruit talent is to stop relying on a person's resume and diplomas and instead focus on their competences, i.e. the combination of knowledge, skills and attitude. This development makes it possible to find potential talent for security in adjacent fields of work such as for instance finance, IT and consultancy. Its use and measure are not yet uniform, but the fields of ICT and Cybersecurity are frontrunners and the EU actively supporting implementing a competence and skills-based approach[17].

A competency is a behaviourally observable combination of knowledge, skills, attitude and/or personal characteristics (personal qualities/capabilities) with which

[9] CBS/HSD (2020). Education and labour market in the security domain - update for the years 2017 and 2018.
[10] https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025
[11] https://www.economicboardzuidholland.nl/deelakkoord-internationaal-talent-programma-ondertekend
[12] https://www.isc2.org/Research/Workforce-Study stating a worldwide gap of 3.4 million cybersecurity workers
[13] Referred is to the five main generations: traditionalists (born 1925 to 1945), baby boomers (born 1946 to 1964), generation X (born 1965 to 1980), millennials (born 1981 to 2000) and generation Z (born 2001 to 2020).
[14] https://longreads.cbs.nl/ict-kennis-en-economie-2022/ict-gebruik-bij-personen
[15] World Economic Forum, Gen Z, and the end of work as we know it, May 2022
[16] https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf states that 54% of organisations struggle to retain talent
[17] https://digital-skills-jobs.europa.eu/en/latest/news/closing-cybersecurity-talent-gap-commission-launches-cybersecurity-skills-academy

certain goals can be achieved. So, it is a combination of three elements: the knowledge (information and experience) a person possesses; the skills a person possesses, i.e., the physical and mental actions that he/she masters well; and the attitudes and character traits typical of a person, i.e., the (mostly learned) attitude a person has towards the world and his/her fellow people. Despite the term 'skills' and 'competences' often being used interchangeably, there is a difference between the two terms. A skill is just one part of a broader competence.

The *European e-Competence Framework (e-CF)*, a common reference for ICT knowledge defines 41 digital competences, all of which can be flexibly implemented, see Figure 3a. It is aimed at ICT professionals and describes general and comprehensive e-Competences, specified at five proficiency or professional maturity levels. These e-Competences can be customised and adopted by enterprises, professionals, and stakeholders in different contexts. As the e-CF only provides examples of job profiles that can be constructed with the framework, the profiles are in fact not a standard but a source of inspiration. Some countries aim to use the profiles more strictly.

The European Cybersecurity Skills Framework (ECSF)[18]. This recent framework aims to create a common understanding of the roles, competencies, skills, and knowledge used by and for individuals, employers, and training providers across the EU, address the cybersecurity skills shortage, and further facilitate cybersecurity-related skills recognition and support the design of cybersecurity-related training programmes for skills and career development. Other than the e-CF, the ECSF fully focuses on and goes into depth on twelve cybersecurity profiles and roles (*see Figure 3b*).

None of the existing collections of job profiles (e-CF, ECSF and securitytalent.nl/career/job-profiles) offer a comprehensive underlying competence framework for the broader safety and security field of work including digitisation. Our conclusion is that there is no such broad scope and widely applicable security framework, those mentioned will have to form the basis.

Figure 3a en 3b: E-CF ICT competence framework and European Cybersecurity Skills Framework job profiles

Dimension 1 5 e-CF areas (A – E)	Dimension 2 40 e-Competences identified	Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3 – 8				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. IS and Business Strategy Alignment			■	■	■
	A.2. Service Level Management			■	■	■
	A.3. Business Plan Development			■	■	■
	A.4. Product/Service Planning		■	■	■	■
	A.5. Architecture Design			■	■	■
	A.6. Application Design	■	■	■		
	A.7. Technology Trend Monitoring				■	■
	A.8. Sustainable Development			■	■	■
	A.9. Innovating				■	■
B. BUILD	B.1. Application Development	■	■	■		
	B.2. Component Integration		■	■	■	
	B.3. Testing	■	■	■		
	B.4. Solution Deployment	■	■	■		
	B.5. Documentation Production	■	■	■		
	B.6. Systems Engineering			■	■	
C. RUN	C.1. User Support	■	■	■		
	C.2. Change Support		■	■		
	C.3. Service Delivery	■	■	■		
	C.4. Problem Management		■	■	■	
D. ENABLE	D.1. Information Security Strategy Development				■	■
	D.2. ICT Quality Strategy Development				■	■
	D.3. Education and Training Provision		■	■		
	D.4. Purchasing		■	■	■	
	D.5. Sales Proposal Development		■	■		
	D.6. Channel Management			■	■	
	D.7. Sales Management			■	■	■
	D.8. Contract Management		■	■	■	
	D.9. Personnel Development		■	■	■	
	D.10. Information and Knowledge Management			■	■	■
	D.11. Needs Identification			■	■	■
	D.12. Digital Marketing		■	■	■	
E. MANAGE	E.1. Forecast Development			■	■	
	E.2. Project and Portfolio Management		■	■	■	■
	E.3. Risk Management		■	■	■	
	E.4. Relationship Management			■	■	
	E.5. Process Improvement			■	■	
	E.6. ICT Quality Management		■	■	■	
	E.7. Business Change Management			■	■	■
	E.8. Information Security Management		■	■	■	
	E.9. IS Governance				■	■

Figure 3a

Figure 3b

Figure 4: Core e-CF competences for Information Security Specialist

E-COMPETENCES

The identified e-Competences for the professional role **Information Security Specialist** are:

Plan	A7	Technology trend monitoring	Level 3-5
	A9	Innovating	Level 4-5
Enable	D1	Information security strategy development	Level 4-5
	D3	Education and training provision	Level 2-3
Manage	E3	Risk management	Level 2-4

Figure 4 shows an application in the digital security field and exemplifies that also non-technical competences are part of the framework. There is a misconception that (cyber)security is all about technical skills and knowledge, this is only partially true.

The European Cybersecurity Skills Framework (ECSF)[19] summarises cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their deliverables, main tasks, key skills, key knowledge and e-Competences (direct link to the e-CF). An example is shown in Figure 5. The ECSF defines more cybersecurity profiles than the e-CF and describes them in more detail and with more attributes but is less of a competence framework and more a list of skills and other attributes of profiles. It gives great insight in what for instance an average Chief Information Security Officer (CISO) should deliver and be able to do and can serve as an inspiration for defining a job at a specific organisation. It does not provide a structured and defined set of skills and levels across all roles that you can create your own profiles or analyse talents with.

A variety of skills-based initiatives

In response to the increasing labour shortages in all sectors, we see many initiatives to promote labour mobility within and between sectors. Scaling up of skills-based tools is an important development to enhance job matches, also in the security domain. The Human Capital Agenda Security (2019 – 2022) already addressed the need to analyse jobs on competence-requirements and the use of 'skills passports' of individuals to facilitate not only job matching, but also upskilling/reskilling, and labour market analysis. The CA-ICT labour market analysis for ICT in The Netherlands, soon to be taken over by NLdigital and PTvT, is experimenting with skills-based analysis of vacancies, for instance in cybersecurity[20]. CompetentNL is a programme that started in 2022 where TNO, CBS, CPB and UWV are working on the development of a uniform

Figure 5: ECSF list of key skills for Cyber Incident Responder

KEY SKILLS

The key skills for a Cyber Incident Responder are:

- practice all technical, functional, and operational aspects of cybersecurity incident handling and response;
- collect, analyse, and correlate cyber threat information originating from multiple sources;
- work on operating systems, servers, clouds, and relevant infrastructures;
- work under pressure;
- communicate, present and report to relevant stakeholders;
- manage and analyse log files.

[18] The final version of the ECSF and its manual were presented at the ENISA cybersecurity skills conference in September 2022: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[19] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[20] https://pr-edict.nl/themarapportages/cybersecurity-2

skills language, also called skills ontology[21]. ESCO[22] is the European initiative for classification of European Skills, Competences, Qualifications and Occupations but still under development for security (armed forces are realised however).

The SEO Economic Research and the Research Centre for Education and the Labour Market (ROA) conducted a survey[23] of skills initiatives in the Netherlands, identifying 43 skills-based initiatives. Their study revealed that the current skills initiatives serve various objectives: developing and using a common skills language; giving insight in and developing personal skills; validation of acquired skills; and matching supply and demand based on skills. Some initiatives are sector-focused (e.g. construction, engineering, healthcare), others regional (metropole Amsterdam, Rotterdam, province of Brabant), or target audience focused (students at vocational education level).

None of the initiatives specifically focuses on the safety and security sector, but various skills initiatives do include security related occupations, such as the occupation Security Specialist ICT in the Dashboard[24] of UWV and SBB[25]. Each profession comes with a list of essential and optional tasks, soft skills and shows whether it is a profession in high demand on the labour market. The mentioned dashboard also shows possible transfers to other professions in higher demand, based on similar tasks and skills.

What does this mean for the security labour market?

With respect to the security labour market, the generic skills-based initiatives a generally not yet usable for security, as we work with specific competences and profiles for occupations in safety and security. At the same time, there is no broadly accepted security competence framework although for cybersecurity steps are taken. This must be taken to the next level: a more complete security competence framework and practical use in training advice and job description. It does not have to be perfect and is no silver bullet but can be made usable as a common denominator to get a better grasp and actionable requirements for people, tasks and training[26].

Validation of acquired skills in a standardised personal skills passport is the ultimate instrument for matching and training, but this is still far away in view of the current multitude of initiatives. The fact that it will take time to establish a standard 'skills passport' does not mean that we cannot work with competence- or skills-based approaches, for instance to attract talent with appropriate competences from other fields of work to switch to a security job. Smaller organisations or those with a smaller digital security team will probably look for a combination of competences in a person to address for instance legal, ethical and privacy matters; or network configuration combined with cybersecurity analysis and -management. As long as fixed job-profiles are not required in a sector or domain and digital security roles don't become protected professions, using a common framework can be even more beneficial for small and medium enterprises.

2.2.3 Talent groups

Based on the previous two paragraphs it is logical to conclude that every talented individual is unique, and they are. At the same time there are groups of talents that are in similar phases of their experience, have certain needs, congregate at certain places, and have career choices to make. They are shortly described here and are used later as part of the intervention matrix.

Primary & secondary education pupils

Primary education focuses on children from ages four to twelve. Usually, children follow primary education for a duration of eight years. Secondary education focuses on children/young adults from ages twelve to sixteen/seventeen/eighteen. Within secondary education the following levels can be distinguished: pre-vocational secondary education (vmbo, 4 learning paths), senior general secondary education (havo) and pre-university education (vwo). Primary & secondary education pupils develop interests in fields that may be their future study and occupation. Depending on their exposure to people and topics this may lead to future digital security professionals. Since most occupations have elements of digitisation and risk management or security in them, it is important that all pupils encounter these topics in an inspiring way.

Vocational education (mbo) students

Secondary vocational education usually takes up four years, depending on the level of training that an individual follows. Mbo courses are given at four different levels of training: level 1 (assistant training), level 2 (basic vocational training), level 3 (professional training) and level 4 (middle-management training). Each level leads to a different job qualification[27]. In addition to the different levels, mbo offers three study forms: BBL, BOL and a shortened pathway. With BBL students go to school 1 day a week and gain experience by working for 4 days. In BOL students go to school for an average of 4 days and do an internship for 1 day to gain practical experience. Shortened pathways are especially interesting for students who already have relevant learning and work experience[28]. For ICT-education, cybersecurity is a mandatory part. Some schools have incorporated elements in other courses such as citizenship for non-ICT students. Working at future employers is an important part of the education, the visibility of work in digital security is unknown.

Higher education students

Tertiary or higher education includes hbo (higher vocational education) and wo (scientific/academic education). These types of education are provided by universities of applied sciences and (general and technical) universities. Both hbo and wo encompass a system of bachelors and masters. Hbo bachelor's degrees take four years, whilst wo bachelor's degrees take three years. Both hbo and wo masters can take upwards of two years to complete[29]. Part-time and modular education from both hbo and wo are growing. Hbo in general is more practical and provides theoretical and practical training for occupations. Wo universities combine academic research and teaching and in general is more theoretical.

Side entrants and Lateral entrants

Side entrants are described as individuals that have followed some sort of (digital security-related) education, but have not been able to complete it, such as drop-outs. These individuals can have the intention of being retrained, through various courses and trainings, to a security-related profession. In schoolyear 2020-2021 nearly 2% dropped out of school (24.385 young people[30]), a big group where, with right support and training, some can be added to the digital security workforce.
Lateral entrants are described as individuals that maintain a parttime or fulltime profession in a non-security-related profession, but have the intention of being retrained, through various courses and trainings, to a security-related profession. Some of these programs do require a diploma

[20] https://pr-edict.nl/themarapportages/cybersecurity-2
[21] https://www.tno.nl/en/healthy/work-youth-health/work-health/skills
[22] https://esco.ec.europa.eu/en/about-esco
[23] SEO, 2 maart 2022, see https://www.seo.nl/publicaties/inzicht-in-skills where the full report and the annex are available in Dutch. The annex contains a tabular overview of 43 skills initiatives. The survey was commissioned by two government departments: Social Affairs and Employment (SZW) and Economic Affairs and Climate (EZK).
[24] https://www.werk.nl/arbeidsmarktinformatie/dashboards/skills
[25] SBB is the Foundation for cooperation on Vocational Education, Training and the Labour Market
[26] Spruit, M. (2022), "Information security education based on job profiles and the e-CF", Higher Education, Skills and Work-Based Learning, Vol. 12 No. 2, pp. 294-308. https://doi.org/10.1108/HESWBL-09-2020-0208
[27] https://www.government.nl/topics/secondary-vocational-education-mbo-and-tertiary-higher-education/secondary-vocational-education-mbo
[28] https://www.kiesmbo.nl/over-het-mbo/leerwegen
[29] https://www.government.nl/topics/secondary-vocational-education-mbo-and-tertiary-higher-education/tertiary-higher-education
[30] https://open.overheid.nl/documenten/ronl-3bcff82b856b8e661f30b7f9443bc6ee46a4062c/pdf

or proven competence. These individuals are also known as ‘career switchers’.

Untapped labour potential

Untapped labour potential includes a broad, diverse range of individuals and groups. Women and minorities are underrepresented in digital security. Since this is such a big group, huge growth can be accomplished here. This target audience also includes individuals that, for various reasons, cannot work fulltime or have difficulty maintaining a full-time job. Furthermore, some individuals within this category maintain some sort of welfare benefit. This includes for example people with a disability, migrants, unemployed individuals, age group 55-plus and recidivists. Groups of refugees and people that are neurodiverse are yet another sub-group.

International talent

International talent includes all internationals that either work parttime or fulltime in a security-related profession or a profession with (some) security-related tasks, and internationals that have the intention of being retrained for a security-related profession in The Netherlands. International talents have unique qualities in the sense that they usually must adjust to the Dutch language and working culture but have the potential to provide different perspectives and background on certain matters.

Working people

The target audience of working people encompasses all individuals in The Netherlands that work either parttime or fulltime in a particular profession. Considering this agenda, we only include individuals that perform at least one specific security or safety related task within their profession or are asked to include them. This pluriform target audience can be found in all Dutch sectors and have a wide array of job titles. This is the biggest group of potential talent for security.

Working security professionals

The target audience ‘workers with a security profession’ encompasses all individuals in The Netherlands that work either parttime or fulltime in a mainly security-related profession. There is no need for these individuals to be retrained for their security function unless they are changing or expanding their role. Instead, it is of importance that there is continuance of ‘life-long learning’ within their security-related profession. We need to upskill current professionals that work in cybersecurity in the new cyber rules and requirements, risk and crisis management. There is a shortage in digital security teachers hindering growth of the talent pool, people with this background and educational skills should be found in this group. Their deployment can also be done in a hybrid form[32].

Key findings from theme ‘Talent’

TALENT 1

The approach towards finding potential security talent may be adapted to:

- identify the specific wishes and expectations of young security talent because of the average higher age in security jobs;
- selectively target and support international talents for work in The Netherlands;
- exploit untapped potential in terms of diversity of the workforce; and
- take special actions to retain security talent.

TALENT 2

Innovative competence- and skills-based approaches can be used to attract and develop talent with appropriate competences, also from other fields of work, to switch or move towards a digital security job. Given the huge quantity of initiatives, we expect that the development of a uniform, standardised competence-based approach will not be a quick fix but necessary next step.

TALENT 3

Each individual and many jobs are unique, but there are clusters and groups with similar properties that can be used for efficient development and targeting of interventions.

2.4 Education

We interpret the theme ‘education’ in a broad sense; it includes formal education and non-formal education, learning and development, training programmes and courses, permanent education, and lifelong development. The theme is closely related to the other themes, in particular Talent, Work and Security. In this section we take a closer look at general trends in education and training; formal and non-formal education in the security domain; and the difference in education between cybersecurity and broader security.

2.4.1 General trends in education and training

The most recent CBS statistics[33] show that in 2018, 58% of all employed persons in a security related occupation had a security related education. In the 2018/’19 school year, 133.000 students were enrolled in a security related programme (11 percent). Higher education level increased from 75 thousand in school year 2013/’14 to 105 thousand in school year 2018/’19. However, at upper secondary vocational level the number of students decreased from 37 to 29 thousand over the same period. Over time the number of participants in security related programmes in Engineering increased from almost 40 thousand participants in school year 2013/’14 to just over 54 thousand participants in school year 2018/’19. In general, we see a trend towards more highly educated security workers and that education of security workers is more often security related. This study does not hold into account the focus of the current agenda, security in a digitising society. A follow-up study is needed to highlight this part (this cannot be done on education titles alone, several studies have tracks with and without attention for digitisation) and update to more recent years. Preliminary analysis of this data shows a growth of digital security students in absolute numbers but also relative to other security students.

Generally, over half of the Dutch workforce between 25 and 65 years followed a work-related non-formal education in 2018[34], making them one of the most active learners in Europe. Lifelong development has become a leading theme for career development and cross-sector mobility. Dutch government has boosted training by providing STAP up until 2023, a subsidy that is available to all employed, self-employed and job searching people in the age of 18 to 67. In a broader learning and development context, we see a trend towards shorter (for instance associate degrees) and modular education (possibly to be combined, also with previous experiences, toward a degree). For example: educational institutions offering separate programmes for study credits and enable taking exams at different levels. The World Economic Forum outlines four trends[35] that will shape the future of higher education: learning from everywhere (immersion); replacing lectures with active learning; teaching skills that remain relevant in a changing world; and using instead of high-stake exams.

Education institute Esade[36] promotes various concepts of innovative learning, for example ‘learning by doing’ and ‘impact learning’, which involve students’ participation in:

- hackathons, datathons, boot camps, outdoor experiences;
- competitions and business games;
- management and decision-making simulations;
- blended courses, which combine classroom training, online experiences and individual study via e-learnings;
- programmes that reinforce conceptual and interpersonal (human) skills: creativity, resilience, critical thinking, communication, collaboration, teamwork;
- solving real-life case studies;
- research projects;
- internships;
- electives from other institutions offered online (as MOOC); and
- other similar intensive learning experiences and challenges.

Some innovative learning concepts are ideally suited for specific target groups, for example: simulations of cyber crises for management/ decisionmakers; hack testing/ red teaming for IT-professionals; and real-life case studies for side- and lateral entrants in digital security.

[31] Cyber Security Raad (2019). CSR Gespreksnotitie Terugdringen docententekort
[32] https://securitydelta.nl/news/overview/pilot-deployment-of-hybrid-cyber-security-teachers-in-technical-vocational-education
[33] CBS/HSD (2020). Education and labour market in the security domain - update for the years 2017 and 2018.
[34] CBS, Adult Education Survey 2018
[35] World Economic Forum, Four trends that will shape the future of higher education, February 2022, https://www.weforum.org/agenda/2022/02/four-trends-that-will-shape-the-future-of-higher-education
[36] https://www.esade.edu/bachelor/en/programmes/double-degree-business-administration-artificial-intelligence-business/why-were-different/learning-by-doing

These innovative learning concepts are also essential for employers, employees, educational institutions, and commercial trainers and certifiers - not only to attract and retain key talent, but also to improve the quality of security work. For instance, improving the cyber resilience of an organisation requires teamwork to cover the three main aspects of cybersecurity: technology, processes, and people. Learning environments such as boot camps, serious games, simulations and challenge-based learning and education can be made very attractive, enjoyable, challenging and effective for the purpose of lifelong development.

Various concepts of innovative learning as outlined above are also applied in security training programmes and events. A good example of immersive learning is the annual International Cyber Security Summer School (ICSSS)[37] and National Cyber Security Summer School (NCS3). The summer schools have put together a highly substantive multidisciplinary program with experts, including challenges, working visits, an HR event with talent matching and social events. The aim of these summer schools is to share knowledge and to discover and develop new talents who are committed or want to commit themselves to digital security.

One of the challenges for digital security and cybersecurity education is the continued scarcity of teachers. Research had been done on a hybrid teacher-solution but letting them work within the school system poses several challenges. Several lessons learned are available[38]. Most require actions on an institutional- or system-level, but teachers themselves can also actively promote contributing to education, connect with external experts and make use of innovative learning concepts.

Learning communities in security

Effective inter-organisational collaborations – often called learning communities (LCs) – translate the latest scientific insights, key enabling technologies and applications, and socio-technical design-expertise proactively into innovative security practices to anticipate potential security threats, ahead of the threat. The two major Dutch security clusters, the HSD and CVD and their affiliated 450+ companies, vocational and higher education institutions, partners, and related security field labs such as Space053 and Impact Coalition for Safety & Security (ICSS) already work for years in LCs for security professionals to address this issue. They have a special focus on cybersecurity and technology in the public security domain (unmanned security systems such as drones, sensors and data analysis, open-source intelligence). The CVD works with big data organisations like Achmea, Tax Office and Kadaster on a system of LC's to enhance uptake of innovations within and between organisations, but also to develop inter-organisational career possibilities. The VNG and police set up a joint programme for leadership in the digital society. Other examples are Living Labs (for instance the IT Forensic Lab of Leiden University for Applied Science), applied research programmes with public-private consortia, peer-learning amongst professionals (such as CISO-sessions) that are often forms of learning communities. The LCs enable security professionals, knowledge institutions and experts from multidisciplinary backgrounds to work and learn together and effectuate an integral Life-Long Learning (LLL) strategy. It reaches big employers, SME's, safety regions, municipalities, police, and education institutes. Research is foreseen[39] to support effectiveness in learning communities.

What does this mean for the security labour market?

The amount of people studying to contribute to security in a digital society both through formal and non-formal education seems to grow but requires better demarcation, research data and analysis to make solid conclusions. Not knowing the size of the problem makes it harder to tune resources and monitor progress. We see a trend towards shorter and more modular education. This makes learning more accessible and efficient, which is good, but holds the risk of not knowing what to choose or combine (for talents and employers) and require or include (employers and educators). There are various concepts of innovative learning, ranging from learning communities to summer schools, that can be made very attractive, enjoyable, challenging and effective for the purpose of lifelong development. Good insights in the effectiveness of learning concepts for this field can make training and education better.

2.3.2 Formal education for the security domain

In the period 2013 to 2018, employed persons in a security related occupation that had a security related education grew from 54 to 58 percent[40]. As mentioned in 2.3.2, preliminary analysis of the data shows a growth of digital security students in absolute numbers but also relative to other security students. Of the graduates in security-related education programmes in 2015/'16, 76 percent found a paid job directly upon finishing their education in October 2016. We expect this to be higher for students in higher education with a digital security profile in that same period. In general, we see a trend towards more participation in higher education, i.e., university of applied sciences, university, and postgraduate programmes. The connection between the different phases and levels of education in security need to be structured well so talents are not 'lost' underway.

Cybersecurity in vocational level IT-studies is already part of the standard curriculum. Many examples show that this topic is also part of higher education studies, also for instance in security studies, law and through minors accessible for other students. There is growing number of associate degrees, bachelor- and master programmes (including professional- and executive masters) that specifically focus on cybersecurity. Their content and scope often differ[41]. The extend to which for instance 'secure coding' is part of a course in coding or system design, is unclear. Education in operational technology (OT), mechanics and autonomous systems like robotics do not include OT-security classes by default, posing risks by future systems.

2.3.3 Non-formal education for the security domain

Commercial trainers and certifiers in digital security (like ISC2, ISACA, SBO, SECO-institute, Security Academy, Fox-IT, Strict, NCOI, Cisco, Hudson Cybertec, Microsoft, KIWA, Signpost Six) report growth in followed training, except for a dip during the COVID pandemic. Combined, private but also public partners (many schools offer professional learning programmes) provide hundreds of courses, conferences, in company training and certifications and educate thousands of professionals each year. A selection of security related education- and training programmes from HSD-partners can be found on www.securitytalent.nl/education.

Training and certification in digital security topics have been around longer than formal education dedicated for this field. Many job postings today require commercial certifications, not formal education titles in for instance cybersecurity. For people that are working or want to enter a retraining program, short and dedicated programs are better accessible. The same goes for employers. There are examples of commercial trainers and certifiers working together with formal education providers and integrating courseware and providing lectures to fill the teacher gap. In general, non-formal education can move quicker in making or adapting their programmes and often have good access to professionals in the field of work.

[37] Security Delta, August 2022, https://securitytalent.nl/news/cybersecurity-talents-broaden-knowledge-during-summer-school
[38] https://securitytalent.nl/news/deployment-of-cyber-security-experts-in-higher-technical-education-key-take-aways-from-pilot-hybrid-teachers report on a study support by Platform Talent voor Technologie (PTvT)
[39] https://www.nwo.nl/en/calls/kic-human-capital-learning-communities-needed-societal-and-technological-transitions-succeed
[40] CBS/HSD (2020). Education and labour market in the security domain - update for the years 2017 and 2018
[41] Inventarisatie van erkende cybersecurity opleidingen in Nederland, PvIB Informatiebeveiliging Magazine, editie 3, 2019

Currently, there is a lack of structure and oversight in formal and non-formal education in the security domain and how they can be combined. There is a huge quantity of education, training, and courses. Ranging in topics from network security to risk management and cybersecurity-awareness. People can no longer see the wood for the trees, Figure 6 shows an overwhelming overview of 473 better known security certifications available in January 2023[41]. The lack of structure hinders people from discerning which offer might match their personal needs.

Most talent is quickly available in the current workforce most training benefits can be made for digital security by investing in this group. They may lack certain knowledge, skills or competencies, but know the practical context where cybersecurity needs to take place and are often close to a position to implement change. Not many of them will do a full year or more of training through formal education. Commercial or internal company training and job engineering can educate this big group. There often are national, regional, employer level and sectoral funding possibilities, such as those provided through UWV and the Human Capital Accord in the province of South-Holland. A broadly available introduction course to raise awareness and interest in a digital security role for young and old, combined with programs such as Alert Online, veiliginternetten.nl, Cyber Security Month and Cyber Security Week, will further support the attraction of new talents if they send a coherent message with actionable intelligence about training and education in relation to tasks, jobs, and personal profile. For people planning to make a career switch to cybersecurity, information needs to be relevant, concise, not to overwhelming and actionable. In 2020 a quartermaster, appointed by the Province of South Holland and supported by the EBZ and HSD[43], analysed the possibilities for an orientation programme to help workers and jobseekers on their way to re-educate or further their skills in the field of cybersecurity. With support of the municipality of The Hague, this resulted in the development of a site[44] for career-switchers towards cybersecurity by HSD.

2.3.4 European initiatives for skills development

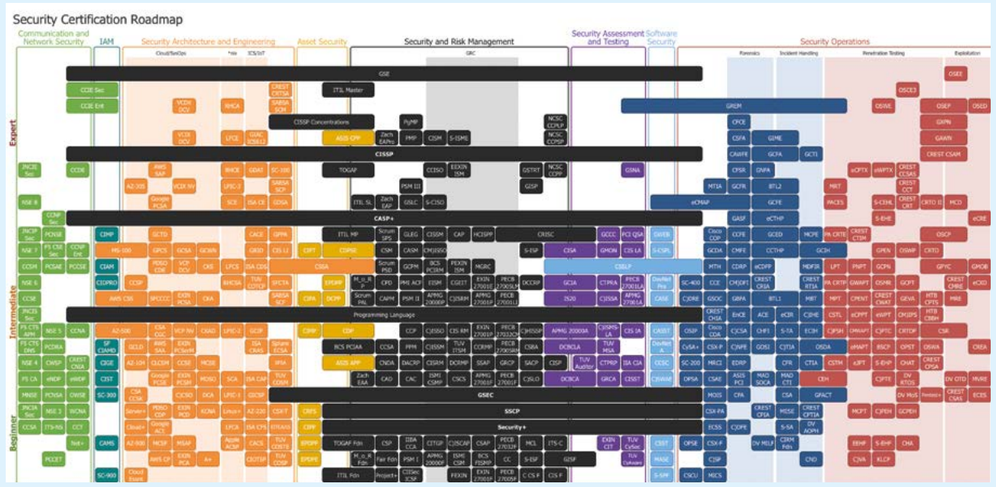
The last few years, the European Union has intensified and set up new actions to support cybersecurity including skills development. The European Cybersecurity Competence Center (ECCC)[45] aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity community. Skills take centre stage in their approach, with the EU Year of Skills[46] and the digital focus of the EU Jobs & Skills platform[47] funded by the Connecting Europe Facility. For individuals and employers, it takes time to find actionable information to direct their skills development and available overviews do not (yet) hold all relevant Dutch actions and offerings. In analysing labour market developments and structuring needs and offerings it is recommendable to keep track of developments and share Dutch initiatives.

2.3.5 Difference between education level for cybersecurity and broader security

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. In contrast, about 76% of the safety & security jobs require a vocational level education in security or do not state any educational requirements at all[48]. 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, a majority of the employers asked for professional certificates in the study from 2018 (there are hundreds of such certificates, see Figure 6 for examples). Employers demonstrate insufficient knowledge of the professional development and career paths of cybersecurity professionals. In fact, they ask for "one or more of the following lists of certificates: (…)". This is then followed by a list, showing certificates that support different career paths. The total list of competences from the analysis 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.

Figure 6: Overview of 473 Security Certifications



[42] https://pauljerimy.com/security-certification-roadmap
[43] https://securitydelta.nl/news/overview/quartermaster-orientation-programme-cybersecurity-me
[44] https://www.cybersecuritywerkt.nl
[45] https://cybersecurity-centre.europa.eu/index_en
[46] https://year-of-skills.europa.eu/index_en
[47] https://www.digitaleurope.org/digital-skills-and-jobs-platform
[48] HSD (2018). Wanted Security Professionals, An Analysis of Job Advertisements. https://securitytalent.nl/career/reports/wanted-security-professionals

Key findings from theme 'Education'

EDUCATION 1
People are getting more highly educated in security and engineering studies are growing their share. The Dutch are relatively strong in Life-Long Learning. New innovative learning concepts provide opportunities for students to be better prepared for the labour market, to add value to lifelong development of security talent and continuous improvement of security work. Learning communities effectuate an integral Life-Long Learning strategy.

EDUCATION 2
The education levels indicated in security job vacancies are indicated with a wide margin, e.g. 'Bachelor or Master'. On the other hand, in job vacancies for cybersecurity professionals, employers often require many specific technical skills, programming languages and certificates.

EDUCATION 3
There is a lack of structure and overview in formal and non-formal education in the security domain, which is a problem for potential talent and employers: how to choose a fitting education, programme, or training? Make sure we don't lose talents underway and relevant security content is part of the programme. Connect with European developments when mutually beneficial.

EDUCATION 4
Make sure that shorter trainings or modules are accessible for workers, they are the biggest group of potential talent. Re-training programs need to be low-threshold and coherent with other studies.

2.4 Work

The theme Work is closely linked to the other themes, in particular Talent (what drives security professionals), Security (what is the content of the work) and Society (how does the security labour market work in The Netherlands). In this section we outline different elements of work: security job profiles; analysis of vacancies and security work in sectors; content, purpose and culture of work; and the recruitment and retention of talent.

2.4.1 Security job profiles

The *Radar for Safety and Security Occupations*[49] shows the inventory and clustering of safety and security occupations ranked by the European Qualifications Framework EQF 1-8. Many professions and their associated job profile descriptions and qualifications were mapped as a first step to contributing to a common set of job profiles for Safety & Security professions, see Figure 7. The profiles are based on established practices in the field, those related to cybersecurity for instance stem from the QIS/PvIB study[50] that on their turn used the e-CF described in 2.2.2. The ECSF-profiles mentioned in the same paragraph can be added or used to replace less relevant descriptions in today's market. The radar of safety and security occupations forms the reference for categorising vacancies on www.securitytalent.nl with one or more job profiles[51]. The profiles can be used for inspiration by employers, who combine elements of different profiles to construct a vacancy text. Some employers have standardised job descriptions with formal frameworks attached and map them on other frameworks or individual talents. Within job profiles, the amount of experience (junior, medior, senior roles for instance) and the context in which the experience is attained also count (size or complexity of the organisation).

Figure 7: Safety and security occupations, HSD, 2018

2.4.2 Analysis of safety and security vacancies

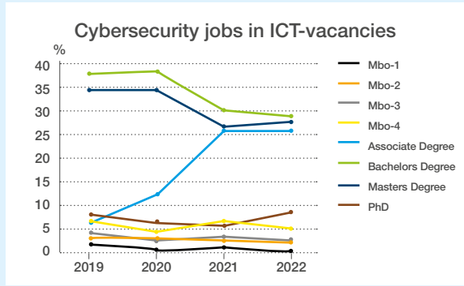
To get an impression of the actual needs and requirements from employers it is good practice to analyse vacancies. Although employers don't always ask for what they need, and texts can be flawed, it is an objective measure. Interviewing employers learned that they find it hard to articulate their needs during interviews and are not very accurate. Vacancies that are not published in open platforms are not measured.

Broader security vacancies

Based on data from securitytalent.nl, we can see several developments in the field of work. In Figure 8 the most required level of education is a bachelor's or master's degree. The growth in associate degrees stems from the fact that vacancies don't require a bachelor of master specifically but 'a higher education degree' (which includes AD's, a two-year programme at a higher education institute).

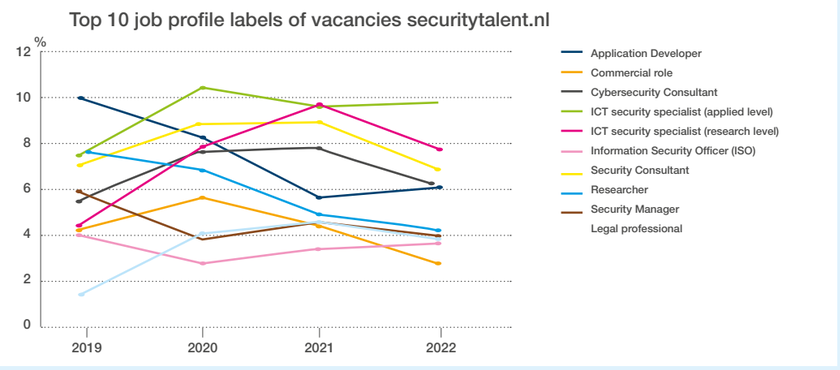
Figure 9 gives an overview of required job profiles and their development in the past 4 years based on securitytalent.nl data. This database of manually classified vacancies listed on securitytalent.nl between 2019-2022 (5,600+ vacancies) has as an advantage that the data is very accurate, disadvantage is that it is not complete (limited to HSD-partners).

Figure 8: Required education level in vacancies HSD-partners



Over the years the demand for ICT- and cybersecurity-talent has been the highest. The commercial- and cybersecurity consultant role are both rather technical. The application developer and research roles are often aimed at automating security tasks or finding other ways of dealing with (cyber)security threats. Since 2019 the absolute number of vacancies more than doubled. There are more job profiles, also those with non-technical backgrounds, but these are lower in demand than the top 10 presented in Figure 9.

Figure 9: Ten most sought-after job profiles in vacancies of HSD-partners



[49] HSD (2018). Beroepenradar Safety & Security. https://securitytalent.nl/nl/nieuws/occupations-radar-for-safety-security
[50] PvIB (2017). Beroepsprofielen Informatie beveiliging 2.0
[51] The latest set of used job profiles are at https://securitytalent.nl/career/job-profiles

Cybersecurity IT-vacancies

From the data derived from pr-edict.nl[52] the number of cybersecurity vacancies is growing in The Netherlands, doubling in the last four years. Also, the number of cybersecurity skills required from ICT-staff is growing, almost doubling in the last four years. The analysis on ICT vacancies is based on Jobdigger's data (excluding vacancies from intermediary organisations), see Figure 10. The definition of cybersecurity jobs and -skills are not given, the cybersecurity filter is within the collection of ICT-labelled jobs.

VPNGids.nl analysed all available vacancies for the period March to September 2021[53] to grasp the current trend in cybersecurity on the labour market. Their most important conclusions are:

- employers seek highly educated personnel (10% vocational education, 70% university of applied sciences, 20% academic level);
- cybersecurity consultancy services require a broad variety of skills including technology, communication, creativity, dealing with complexity, problem solving;
- relevant experience counts: the word 'senior' occurs almost 2.5 times as often as 'junior' in vacancies, while the total number of juniors, trainees and interns is lower than the number of seniors;
- the demand for ethical hackers doubled;
- the business community also looks for negotiators in ransomware cases;
- the average salary is € 4,000 gross per month, which is relatively low given the scarcity; and
- a very large share of cybersecurity vacancies in government comes from the police.

Compared to other countries, the relative amount of people working in cybersecurity jobs in The Netherlands is rather low. When combining the ISC2 2021 Workforce Study with OECD Workforce size statistics, you can see that we have one of the lowest percentages compared to other western digitised societies (*see Figure 11*).

There is a lot of research done on labour market statistics in security, cybersecurity, and ICT. Insights are getting better but there are still a lot of unknowns and diversity in demarcation. Standard labour market statistics don't have the details needed to pinpoint actions on. Starting in 2023, a new study is foreseen on cybersecurity commissioned by the Ministry of Economic Affairs.

Figure 11: Estimate number of cybersecurity staff as part of workforce

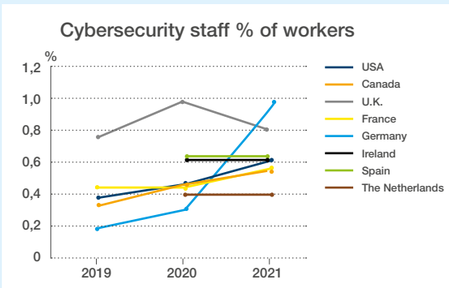
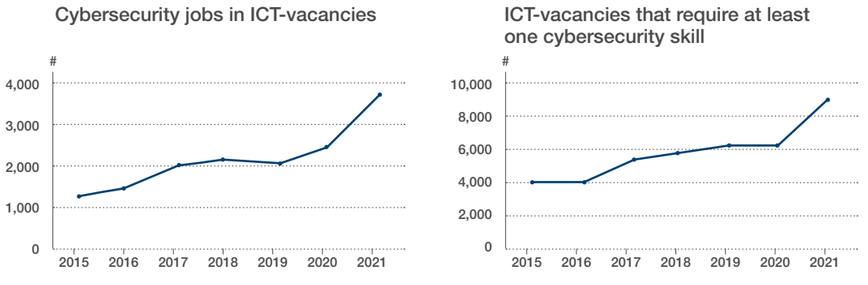


Figure 10: Demand for cybersecurity talent and skills in The Netherlands, CA-ICT, 2022



[52] https://pr-edict.nl/themarapportages/cybersecurity-2

[53] VPN Gids, October 2021, https://www.vpngids.nl/nieuws/onderzoek-cybersecurity-arbeidsmarkt-nederland

2.4.3 Security work in sectors

In 2018, 13.2 percent of the Dutch workforce (1,158,000 people) was employed in a security related occupation: a growth of 80,000 jobs[54]. Other relevant conclusions from this research:

- 43% of all security occupations were in Health & Social Work (22%) and Public Administration & Services (21%) (year 2018).
- The number of employees in security and security related professionals is largest in the Information & Communication sector (49% of all persons employed in this sector) and in Public Administration & Services (48% of all persons employed in this sector).
- The distribution of jobs in the security domain across branches of industry is relatively constant over time. In terms of the number of security jobs (both primary and secondary security jobs), the largest branches are, in order, Health & Social Work, Public Administration & Services and Information & Communication and this order remained relatively constant since 2013.

The top sectors for new digital talent is different but not yet researched. There are some dominant sectors, but in general technical talent work in many different sectors. Employers can strengthen the security field by giving a good example of how to contribute to security, make security important ('chef sache') and get the basics right[55]. An intersecting group of employers are Small- and Medium Enterprises (SME's). They are active in almost any sector but share some specifics hindrances regarding cybersecurity talent. Because of the smaller size and often limited IT-personnel, their attention to cybersecurity and skills development in general is limited. Research by a quartermaster commissioned by the Economic Board South-Holland and HSD that was concluded in 2023[56], showed the lack of ownership of cybersecurity tasks in SME's. It resulted in an 'Instrument Human Capital Cybersecurity' to support businesses that need to implement cybersecurity plans.

Distinction between 'primary security' and 'secondary security' occupations

More and more elements of safety and security occupations are dedicated to security to guarantee the continuity and integrity of business and IT systems and protect against cybercrime and fraud. To give some distinction in this broadly defined security domain, occupations can be classified as: 'primary security' or 'mainly security related' if 50% or more of the tasks is dedicated to security; and 'secondary security' or 'partially security related' if 10% to 50% of the tasks is dedicated to security. To get a more accurate number for required security skills and potential training needs, this should be further refined in the future.

2.4.4 Content, purpose and culture of work

Three essential characteristics of work (other than salary, job security, flexibility, development opportunities, autonomy and location) are: content, purpose and work atmosphere or culture[57]. These are important for anyone working, seeking work or looking for other work, and are different in security and can be altered by employers in this field:

- **content:** the set of tasks, activities, roles and responsibilities that characterise a particular occupation, function and/or position in an organisation;
- **purpose:** the objectives of a particular type of work within a particular organisation, that which makes the work at this organisation meaningful in the perception of the worker - meaningful often from a social point of view;
- **culture:** the work atmosphere and culture within an organisation - both the physical workplace, working conditions and the set of values and beliefs, leadership, cooperation, attitude and behaviour, customs and habits, which make the organisation either a great place to work, a terrible place to work or any nuance in between.

2.4.5 Recruitment and retention of talent

Interesting, attracting, recruiting and selecting potential talent is a management responsibility, often delegated internally to Human Resource (HR) or Recruitment or outsourced to an external recruiter. In these times of unprecedented staff shortages, traditional recruiting via posting vacancies does not always suffice. New insights collected from an array of sources on recruitment are:

- embedding recruitment in broader labour market communication with the intended target group(s) via continuous presence on social media, in trade

[54] CBS/HSD (2020). Education and labour market in the security domain - update for the years 2017 and 2018

[55] https://vng.nl/sites/default/files/2020-02/vng_agenda_digitale_veiligheid_2020-2024_def.pdf

[56] Cybersecurity binnen het mkb: met welke human capital aspecten moet je rekening houden? https://securitydelta.nl/news/overview/cybersecurity-within-smes-what-human-capital-aspects-to-consider

[57] https://www.nationaleberoepengids.nl/werkgever-beoordelingen-in-2020

magazines, at training courses and events;
- building long-term relationships with potential candidates and alumni;
- enticing potential candidates to attend a master class, learning game (serious gaming) or participate in a challenge;
- tempting potential candidates to visit open days, where they can informally get to know the organisation, the work, the team and the culture;
- having an eye for what is called 'the candidate experience';
- using AI to track down and select potential candidates; and
- recruiting based on skills and potential rather than diplomas and experience.

After the recruitment and onboarding process, talents and employers can benefit from an employee development plan to support their development in the organisation and the field of digital security. Younger generations in general are less bound to the employer and the field of work. Over-specialisation and differentiation may hinder their sense of belonging, career development and purpose, making retention and guided development more important.

> *"Traditionally, the focus is on experience, but you can also look at someone's potential. Then it's about curiosity, drive and analytical ability, for example. If someone scores high on these, they will develop quickly. That person may come from further away but can also go far."*

What does this mean for recruitment on the security labour market?

Both the broader marketing-like approach of recruitment and the above approaches that work are general in nature, but certainly also relevant for the security labour market. The COVID pandemic increased the mobility of employees between sectors ('cross-sector mobility'), which means that the war for talent is being fought in a wider area than the security sector and adjacent sectors alone. Side entrants with the right skillset can be persuaded to work in a security profession provided the different job profiles are clear, the career perspectives and overall employee value proposition attractive, and the employer delivers what is promised. Examples of recruitment innovations in IT and security include:
- the pilot of the Municipality of The Hague, in which around a hundred higher educated unemployed people were trained as cybersecurity consultants and deployed to advise small and medium size enterprises;
- the unique IT orientation programme for career switchers with or without any background in IT (Techgrounds); during the Pathways programme, potential candidates match their skills, talents, and past experiences to either upskill or start a successful career in IT[58];
- the talent acquisition platform for vocational level (mbo) graduates and students Play-to-Work that helps recruiters and employers to search, find and prequalify candidates for vacancies[59].

Need for technical and non-technical competences

Generally, we see that technology has a huge impact on operations in the security domain. This is reflected by the request for security talent with an engineering background and at the same time many people in working in cybersecurity with a non-IT background. There are opportunities for non-technical staff to work in security and security related occupations, but the wide-spread request for them is not visible in job openings. People without a typical technical education can be empowered to train themselves (for example via MOOCs, subsidised programmes, or company- and sectoral training programmes), re-skill, up-skill, and embrace a life-long learning attitude to enhance their competences for the security domain. In addition, all people should become more aware of technology, digitalisation, the impact of artificial intelligence and cybersecurity risks. At the same time the topics that were traditionally more technical in nature get a broader scope including business and personal behaviour.

[58] https://techgrounds.nl/pathways-english
[59] https://playtowork.nl

Key findings from theme 'Work'

WORK 1
Job profiles within the safety and security domain are diverse but can be used for inspiration and classification of functions. Many more jobs contain security- and cybersecurity tasks, how many and to which amount is not known.

WORK 2
The required security talent is mostly technically schooled and have higher education level training. The demand is growing, doubling in the last 4 years. Technical, commercial, automation and innovation skills are in high demand. Problems are big and urgent. The current percentage of the workforce in cybersecurity is low compared to other countries, further growth can be expected.

WORK 3
In these times of unprecedented staff shortages, traditional recruitment approaches are less effective. New marketing-like approaches may also work to attract and retain security talent, which includes mainly security related occupations, often within the security sector, and partially security related occupations, often in other sectors. Work is more than a collection of tasks, purpose and culture attracts and retains talent.

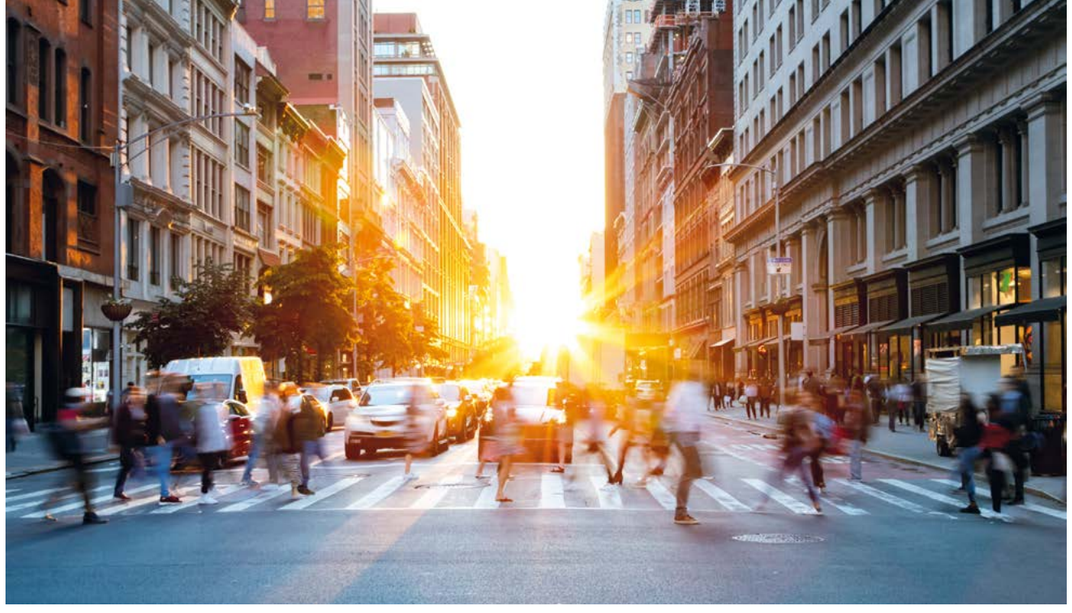
2.5 Security

In this section we reflect on safety and security developments that impact the need for talent. We set out the increasing attention for digitalisation and cybersecurity in the security domain, discuss the Dutch Cybersecurity Strategy for the coming years and its impact on talent. Developments in business continuity and risk management are addressed shortly, before taking a look at changing EU regulations in the field of (cyber)security.

2.5.1 Increasing attention for digitalisation and cybersecurity in the security domain

Security is of great importance for people, companies, organisations, the government, and society at large. For people, the need for safety and security is key, both in the physical and digital domain. In companies and organisations, a cyber-attack can be a downright threat to the continuity of business operations, their awareness and practical support are therefore focus points for the Digital Trust Center[60]. But digitisation can also support efficient performance of security tasks and new security related products and services. For the government, security is not only essential to protect vital infrastructure, but also the democratic system, rule of law and public values. For society at large, fighting crime and promoting security is an essential condition to function well. Various initiatives indicate increased interest in digital aspects of safety and security. Three examples in this respect are described here.
- Research conducted in 2020 shows that digital knowledge and skills have become increasingly important for police work[61]. This research clarifies the digital aspects of police work and the digital knowledge and skills gap within the police force. In addition, it provides insight into how this knowledge and skills gap can be closed.
- The Center for Security & Digitalisation, CVD, has a wide range of personalised learning paths around digitalisation and security through its knowledge partners. At every level (prospective) professionals can get to work on the issues at hand. Young talent can make the step to the security domain through specialised full-time studies. For students and professionals, there are short-term minors and modules to sharpen their knowledge. And masters offer the opportunity to delve deeper into complex security issues.
- Topsector ICT strengthens the economy with innovations by exploiting international opportunities, solving societal

[60] https://www.digitaltrustcenter.nl
[61] PIAC, Level Up, Knowledge for police work in a digital society, July 2020



challenges, increasing human capital, and investing in scientific research. Five key technologies have been put on the agenda: big data, AI, blockchain, Future Network Services and cybersecurity. All of these are relevant for security in a digitising society.

We identify various trends and developments in the field of security such as geopolitical tensions that effect businesses, growing collaboration and dependencies between organisations, the rise of new technology - quantum, artificial intelligence, drones, internet of things - each with their own security challenges, the shift from 'traditional' forms of crime to cybercrime including cyber warfare, the increased economic importance of ICT and the rapidly increasing spread of disinformation via social media. Section 2.6.2 discusses the technological developments that have an impact on safety and security further.

There is a growing collaboration between organisations to deal with security threats related to the digitalisation of society. Great examples to improve cyber resilience are Cyberweerbaarheidscentrum Greenport[62], FERM-Rotterdam[63], Centre for Safety and Digitalisation[64], Digital Trust Centre, dcypher and Security Delta. The agendas of the National Coordinator of Counterterrorism and Security (NCTV) of the Ministry of Justice and Security[65], the National Cyber Security Center (NCSC)[66] and the monitoring of cybersecurity and security by Statistics Netherlands (CBS)[67] exemplify the relevance of security in a digitising society.

2.5.2 The Netherlands Cybersecurity strategy 2022 – 2028

In October 2022, the National Coordinator for Counter-terrorism and Security (NCTV) published the cybersecurity strategy[68] for the upcoming years. The fourth pillar of this strategy identifies two priorities most relevant to this Human Capital Agenda: first, making digital resilience part of the education curriculum in primary and secondary education; second, focusing on the cybersecurity labour market. These goals are further broken down into seven actions in the accompanying action plan[69]. The government is working with educational institutions on upskilling and retraining programmes to increase workers' cybersecurity expertise. To this end, they are working with the business community and other relevant parties. This will include identifying bottlenecks and restrictions in that cooperation arising from regulations, and considering what solutions are needed for them. The government aims to invest in higher vocational education programmes in science and technology, of which cybersecurity programmes are also a part. Resources are deployed on (1) higher intake within the study programme, (2) lower dropout and switch, (3) higher lateral intake, (4) induction/warm transition from study programme to labour market.

The other pillars include cybersecurity-related developments that will have an impact on work. In general, organisations need to strengthen their resilience, growing the need for talent. Products and services need to be more cybersecure (more secure development) and knowledge and innovation need to be strong (good research). Digital threats by state actors and criminals need to be monitored and managed, government has a special responsibility in this pillar (more capacity needed).

2.5.3 (Cyber) security, risk, business continuity and crisis management

The scope and impact of security has broadened over the last decades, as follows:

- the rise of Business Continuity and Crisis Management;
- the rise of offensive cybersecurity actions by various state actors to influence and interfere with Dutch interests[70];
- the further development of Risk Management into mature risk awareness, detection, management and control systems, supported by technology, such as dashboards;
- the integration of cyber risks into general risk management frameworks (adding cyber to strategic, operational, financial, IT and other more traditional risk areas). Cybersecurity measures are implemented more frequently into the risk management framework of large organisations than small organisations[71];
- the shift from risk aversion to resilience; and
- the enforcement of the GDPR (privacy regulation).

What does this broadening of scope mean for security talent, education and work?

The broadening scope of security and the increasing attention for digitalisation and cybersecurity in the security domain, has an impact on the other themes Talent, Education and Work. Talent faces more career development opportunities, for instance more choice between different career paths that are still under development (not yet 'set in stone'), and need competences for security in the digital domain. Education faces the challenge of incorporating conceptual risk thinking and technology into their graduate and post graduate programmes. With respect to the theme Work, the broadening scope needs to be translated into competences - knowledge, skills, attitude and behaviour - and be added to professional profiles, which in turn has an impact on training and upskilling requirements. Obviously, all these developments taken together influence the labour market for security talent.

2.5.4 Changing EU regulations on (cyber) security

The Digital Europe Programme[72] aims to help the EU achieve a high common level of cybersecurity. Several European directives and regulations on cybersecurity are already in effect and others are on the threshold of being implemented. These are expected to have a serious impact on security, the way we do business and need for talent. Amongst other, the need for supervision, certification and auditing will grow. This requires different knowledge and skills, for instance auditors with more cybersecurity knowledge or cybersecurity- and legal professionals with more auditing skills.

EU Network and Information Security Directive

Better secured network and information systems and a reporting obligation for serious cyber incidents should significantly increase digital security in the European Union (EU). Key players in the food sector (industrial food production and distribution such as larger supermarket chains), but also parties in the chemical and manufacturing industries, waste management, postal and courier services and data centres will have to start taking appropriate cyber measures from mid-2024. EU member states and the European Parliament reached a political agreement on NIS 2 in June 2022[73].

From mid-2024, the number of sectors will be greatly expanded. The revised NIB2 directive will then have two categories: essential providers and major providers. With essential providers, mainly parties from Dutch vital sectors, supervision will soon be proactive. With key providers, supervision takes place after the event, if there

[62] https://cwgreenport.nl - launched October 2022
[63] https://ferm-rotterdam.nl
[64] https://www.cvdnederland.nl
[65] https://www.nctv.nl
[66] https://www.ncsc.nl
[67] https://www.cbs.nl/nl-nl/longread/rapportages/2022/cybersecuritymonitor-2021 and https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021

[68] NCTV (2022). Nederlandse Cybersecuritystrategie 2022-2028. https://www.nctv.nl/actueel/nieuws/2022/10/10/nieuwe-cybersecuritystrategie-met-ambities-en-acties-voor-een-digitaal-veilige-samenleving
[69] NCTV (2022). Actieplan Nederlandse Cybersecuritystrategie 2022-2028. Pages 48-51. https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028
[70] NCSC (2022). Nederlandse Cybersecuritystrategie 2022-2028. Page 7
[71] https://www.cbs.nl/nl-nl/longread/rapportages/2022/cybersecuritymonitor-2021/2-cybersecuritymaatregelen
[72] https://digital-strategy.ec.europa.eu/en/activities/cybersecurity-digital-programme
[73] https://www.nis-2-directive.com

are indications of an incident. These are mainly (medium) sized parties, where disruption will not have very serious social or economic consequences. Besides the reporting obligation, all providers that will be covered by the revised directive must also start taking security measures; the so-called 'duty of care'. These include increasing the security of their supply chain and getting the way cyber incidents are handled in order.

EU Critical Entities Resilience Directive

In July 2022, the EU member states, the European Commission and the European Parliament agreed on a European CER Directive[74]. This directive will protect providers of vital processes by increasing their resilience. This will better safeguard the continuity of these processes. The directive focuses on the physical safety and security of vital processes such as drinking water supply and energy. Together with NIS 2, the CER Directive provides a framework for digital and physical resilience of vital providers. In doing so, the directives strengthen the foundation of physical and digital security, ensuring a resilient economy and society both in The Netherlands and the rest of the European Union.

This new directive covers more sectors than just energy and transport, as was the case with the old directive. New sectors include food supply, healthcare, financial market infrastructure, drinking water, digital infrastructure, wastewater, public services, banking, and space services. The directive also extends rights and obligations of vital providers.

EU Cybersecurity Act

The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes[75]. The act grants a mandate to ENISA (the EU Agency for cybersecurity) to set-up and maintain the EU cybersecurity certification framework by preparing the technical grounds for specific certification schemes. The cybersecurity certification allows companies doing business in the EU to only have to certify their ICT products, processes and services once.

Digital Operational Resilience Act

From 2025, financial institutions must comply with the Digital Operational Resilience Act (DORA). The Digital Operational Resilience Act offers an integrated approach to managing ICT risks. The new European legislation was created in response to the increasing digital dependency of companies and the increasing threat of cyber-attacks and data breaches.

EU Cyber Resilience Act

The EU Cyber Resilience Act (CRA) is a legislative proposal, still in progress and has not yet been implemented into EU regulations, to implement cybersecurity regulation to ensure more secure hardware and software products. Currently, such products suffer from two problems. First, hardware and software products generally contain a low level of cybersecurity. Second, there is an insufficient understanding by users to securely utilize and choose these products. The CRA sets out two objectives to ensure proper cybersecurity regulation:

1) Create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and
2) Create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

EU Cyber Solidarity Act

The EU Cyber Solidarity Act is a proposal by the European Commission to improve the preparedness, detection and response to cybersecurity incidents across the EU[76]. The proposal includes a European Cybersecurity Shield, made of Security Operation Centres interconnected across the EU, and a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber posture. The act is still in progress and has not yet been implemented into EU regulations.

[74] https://www.critical-entities-resilience-directive.com
[75] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[76] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

Key findings from theme 'Security'

SECURITY 1
Security, both in the physical and digital domain, is of great importance for people, companies, organisations, government, and society at large, and in view of the ongoing developments we expect this importance to increase rather than decrease.

SECURITY 2
The scope and impact of security has broadened over the last decades to include topics such as cybersecurity, business continuity, crisis management, and integration in general risk management frameworks. This broadening scope has an impact on Talent, Education and Work and taken together, the labour market for security talent.

SECURITY 3
Digitalisation and cybersecurity are in the spotlight within the security domain. New technologies can support efficient performance of security tasks but also threaten security and increase cybersecurity risks. There is a growing collaboration between organisations to deal with security threats related to the digitalisation of society.

SECURITY 4
Several European directives and regulations on cybersecurity such as NIS-2, DORA and CRA, are already in effect and others are on the threshold of being implemented. The need for supervision, certification and auditing will grow and will require different knowledge and skills.

2.6 Society

In this section we discuss the key trends and developments in society that affect the work in safety and security. We focus successively on the following areas: developments on the labour market including presence of women; technological developments that affect safety and security; social trends; international level risks; and regulatory tightening.

2.6.1 Developments on the labour market

It has recently become clear that the Netherlands is facing major personnel shortages[77] in almost all sectors. There are huge shortages of security guards, IT professionals, staff in engineering, construction, healthcare, education, police, etc., which have a major impact on the day-to-day operation of business and services and are potentially disruptive for society. This is against the backdrop of bigger changes on the labour market[78], such as the increase of flexible labour, growing influence of technology on work and growing complexity. These each pose security challenges and require different competences.

An analysis of general staff shortages

One structural cause is the demographic development of the working population in The Netherlands: ageing of the current workforce together with declining numbers of new entrants on the labour market. Another structural cause is the fact that more and more young people are opting for higher or theoretical education, resulting in a decrease in the number of students in intermediate vocational or practical education. This while the demand for practically trained professionals is rising sharply, in particular in the energy transition and construction.

Recently, the Research Centre for Education and Labour Market updated their July 2021 report, with a specific focus on forecasts for the expansion demand[79]. The economy is now expected to grow faster the coming six years than anticipated in last year's publication. Although the job openings are still mainly driven by the replacement of staff, the higher expected economic growth now means that 1 in 5 job openings is due to job growth. This results in persisting and increasing staffing bottlenecks in science and engineering, healthcare, and education on all educational levels. Even though the economy seems to recover well from the COVID pandemic, the current high inflation, escalating energy prices and possible recession might cause economic growth to be hampered in the coming years[80].

[77] https://www.cbs.nl/nl-nl/nieuws/2022/33/spanning-op-de-arbeidsmarkt-loopt-verder-op
[78] WRR (2020). Het betere werk. De nieuwe maatschappelijke opdracht

Untapped labour potential

UWV and CBS provided new insight into the composition of untapped labour potential: how many and which people are available to work or work more hours? Their report 'Composition of unused labour potential' answers the question which jobseekers are potentially available for 'hard to fill' vacancies[81]. Despite the record shortage, there is still a lot of unused labour potential. According to the CBS, this group of unemployed, semi-employed and underemployed part-timers consisted of 1,114,000 persons in 2020. Of these, only 29% were registered as jobseekers at the UWV.

Women in beta, tech, engineering and IT

The Minister of Economic Affairs addressed gender diversity and inclusiveness in a recent letter to Parliament[82]. Inclusiveness is an important area for improvement for beta, technical, engineering and IT companies. The influx of women in Science - Technology - Engineering - Mathematics (STEM) is significantly lower than the influx of men. Women with a technical education switch more often to non-technical professions (5.6%) than men (2.9%). VHTO, the Expertise Centre for Gender Diversity, published the whitepaper[83] *Women in beta, engineering and IT - how do you retain them as an organisation.* VHTO mentions four main reasons why women quit beta, tech, engineering and IT jobs: gender bias in the workplace; low confidence in own abilities; combination of work and care responsibilities (work-life balance); and not feeling at home in a male-dominated company culture. Furthermore, VHTO outlines ten concrete actions[84] companies can take to attract and retain women. In the security domain and in cybersecurity functions the problem is no different, research showed that women in cybersecurity account for roughly 24% of the workforce[85].

2.6.2 Technological developments

Technological developments affect safety and security, such as:

- the rapidly increasing digitalisation: automation of processes and systems, robotisation of production and distribution, the use of connected smart services (Internet of Things, IoT, cloud services), quantum, blockchain, and numerous applications of AI, virtual reality and augmented reality; and
- the exponentially increased availability of data, the possibility of comprehensive data and scenario analysis as a basis for responsible decision-making in complex cases - in brief: data driven analysis and decisions.

Many of these developments did not start in security or are not limited to it. Their development is probably hard to stop if you would like to. Directing their application and limiting their possible negative impact on security is in our hands. All these technologies impact the work in security, not only changing security but also the required work. Some technologies can be used to automate or support security workers to deal with shortages, the rise of Generative AI can have its benefits for security but it also heightens cyber threats such as phishing and identity fraud which add to the workload of overstretched cyber teams.

2.6.3 Social trends

We notice increasing societal tensions and threats due to an accumulation of different developments, taking place in the physical and are facilitated by the digital world:

- various short-term and long-term crises - energy, workforce, housing, immigration/refugees, poverty - so complex that they cannot be solved easily by government, businesses, and citizens;
- ongoing individualisation in western culture;
- perceived inequality between people (the '*haves*' versus the '*have nots*');

A FEW EXAMPLES OF TECHNOLOGICAL INVESTMENTS IN SECURITY

- the use of surveillance cameras in public spaces;
- the use of crowd management data at big events;
- the use of facial and voice recognition systems during high-risk football matches;
- the use of Artificial Intelligence (AI) to support decision making;
- the use of threat intelligence data for Security Operation Centres;
- the use of AI to automate threat analysis;
- the use of AI to track down cyber criminals;
- the use of algorithms to detect fraud;
- the use of robots to explore a potentially unsafe environment; and
- the use of drones to deliver rescue material.

[79] ROA (2022). https://roa.nl/news/update-labour-market-prospects-2026
[80] ROA (2022). Factsheet. https://roa.nl/files/roaf20223arbeidsmarktprognoses2026pdf
[81] https://www.werk.nl/arbeidsmarktinformatie/prognose-trends/wie-zitten-in-het-onbenut-arbeidspotentieel
[82] Letter dated 15 July 2022, Addressing labour shortages for the climate and digital transition
[83] https://www.vhto.nl/kennis/whitepaper-behoud-vrouwen-in-tech/

- increasing polarisation, conspiracy thinking, separation of social groups, often fuelled by social media, for example during the covid pandemic;
- a decreasing trust in the government, the established institutions, perhaps even the democratic system;
- frustration and anger that expresses itself in personal threats to political office holders, politicians, police, ambulance personnel, doctors, scientists, and journalists;
- generally, a reduction of tolerance in society.

2.6.4 International level risks

The future is uncertain, we live in a 'VUCA'[86] world. The development of the economy is difficult to predict because of its interconnectedness with, and dependence on, events and developments with a global impact, for example:

- the COVID pandemic;
- climate change leading to droughts, floods, forest fires of extreme magnitude (and consequent crop failures, poverty, migration);
- the war in Ukraine affecting the supply and pricing of oil and gas from Russia in unprecedented ways; and
- the dependence on technology, energy and global supply chains.

The ongoing uncertainties, vulnerabilities, complexities, and ambiguities have a great impact not only on society at large, but also on our safety and security and potential security talent. Megatrends and macroeconomic developments create uncertainty. This raises the question of which security issues remain valid regardless of the economic climate, even in times of recession. Issues such as: automate security internally or outsource externally; how big is the sustainable shortage of security professionals? Since the cybersecurity shortage was identified long before the current tight labour market and the work population is aging, we expect the shortage remains valid regardless of the economic climate.

2.6.5 Regulatory tightening

Finally, government and organisations must deal with regulatory tightening, such as the implementation of new European Directives (discussed in detail in Paragraph 2.5.4. The generic social development is that there are more rules and more uncertainty about their enforcement and remaining risk profile. Police and Public Prosecution Service, but also municipalities and the Dutch DPA, have more work than they can execute. Not all rules and regulations receive the same amount of attention and execution power, at the same time their number grows, and penalties do as well. This has an impact on both expected protection and adherence to rules and regulations.

Key findings from theme 'Society'

SOCIETY 1
There are huge staff shortages in all sectors which also affect safety and security. At the same time, there is a large untapped potential in the labour market, i.e. people who are available to work or work more hours. Gender diversity and inclusion is a well-known issue.

SOCIETY 2
Technological developments, in particular digitalisation and the availability of data, influences safety and security twofold: an increase in opportunities - such as investments in technology, AI, etc. – and in threats – such as more forms of cybercrime.

SOCIETY 3
Increasing social tensions and ongoing concerns about developments impacting the economy have an influence on safety and security and the need for well-trained security professionals.

SOCIETY 4
Government and organisations must deal with regulatory tightening. Not all rules and regulations receive the same amount of attention and execution power, at the same time their number grows, and penalties do as well.

[84] https://issuu.com/vhtoamsterdam/docs/print_vhto_10_inzichten_los
[85] https://www.isc2.org/Research/Women-in-Cybersecurity
[86] The acronym VUCA stands for: Volatile, Uncertain, Complex & Ambiguous

3. Action plan

3.1 HCA Security execution

In this chapter, we describe action lines inspired on the key findings in five connected perspectives from Chapter 2: Talent, Education, Work, Security and Society. Action lines are realised through one or more actions or activities. Examples of these actions are given in here and further in Chapter 4. The key findings from Chapter 2 are linked to or the origin of actions, the matrix for actions and key findings can be found in Appendix 3 – Matrix of actions and key findings. Based on trends and developments, opportunities and threats, we added and will add new actions in the future if needed. It is a 'rolling' agenda. By combining and connecting initiatives by others or in other fields that deserve scaling up, we can realise more results.

As regards to new actions, we will focus on solutions, approaches and interventions that have proven effective and are possible to scale. We will support actions that contribute to growing the pool of security talent, both in 'mainly security-related' functions and 'partially security-related' functions. We will walk different paths to achieve availability of talent, by growing the scale of actions, getting a bigger mass, reduce the time to results and combining goals in single actions. This means that the actions mentioned below under one of the action lines are likely to serve more than one.

Regarding the execution and funding of the actions, this is something that is already arranged for some but certainly not for all actions. Some actions and interventions (*see Paragraph 4.2*) are also part of other and related initiatives[87].

3.2 Better functioning of the labour market

To contribute to a better functioning of the labour market for digital security, several actions need to be taken that affect different perspectives: Talent, Work, Security & Society.

3.2.1 Support HR professionals

The extremely tight labour market, with staff shortages in all sectors including the security domain, requires smart, tailored, unconventional approaches. In Chapter 2 we discuss recent insights into the recruitment of talent, outline approaches that work, provide examples of successful interventions in IT/security and elaborate on security occupations. Further building on previous initiatives for HR-professionals, we want to support them in the security domain in various ways.

Proposed actions:
Organise a series of knowledge sharing and networking events and tools for recruitment and HR around topical issues in the field of talent, work and security, in order to:

- attract younger generations;
- attract a more diverse workforce;
- attract potential talent, currently part of the untapped labour potential;
- explore job engineering/ job enrichment in digital security, offer personnel with ambition to grow into this area or have adjacent tasks a development path, guidance and training.

Action described in detail: Attract younger generations
To attract generation Z, both the communication style and the job offer within the security work domain (also referred to as 'the employee value proposition') must be tuned in to their values, beliefs and expectations. Actions may include the definition of (a) preferred work requirement(s) for younger generations in close cooperation with the target audience (from different education backgrounds); and preferred communication styles to approach the target audience.

Action described in detail: Attract a more diverse workforce
Building upon the concrete actions of Expertise Centre for Gender Diversity, employers of security talent may boost the attraction and retention of women by:

- enhancing visibility of women at work in security a.o. via the two talent platforms securitytalent.nl and cybersecuritywerkt.nl;
- sharing best practices on attracting and retaining women (role models, network opportunities, safe and pleasant

[87] For instance 'Actieplan groene en digitale banen' and the 'HCA-ICT'

work environment, work-life balance choices, inclusive performance appraisals); and
- enlarging the pool of potential security talent by connecting coaches, mentors, and other ways supporting women who are interested to work in security.

Action described in detail: Tap into the unused labour potential

To attract talent currently part of the untapped labour potential, Techgrounds[88] helps with reskilling to IT by providing an easy access, free of charge, orientation programme for people who are interested in IT, regardless of their level of education, and with a job guarantee for those who graduate the Techgrounds Academy. Although it is a successful initiative, the programme is fulltime, which is not always feasible for many belonging to the group 'the untapped labour potential'. We realise that this group is very diverse (disabled, migrants, age group 55-plus, all people who cannot work fulltime for whatever reason). Employers can fill more vacancies from the untapped potential by being creative and flexible (and not asking the impossible). For instance, by adjusting work schedules, setting different job requirements and by training people themselves. UWV and municipalities, together with employers, can help jobseekers find and re-skill for a more promising occupation.

Given the huge tightness in the labour market, it is important for employers to know how to retain their employees and prevent people from dropping out, but also to seize opportunities to help people who currently do not have a job find employment. This requires more than good pay and working conditions. Reducing work pressure, offering education and training, providing opportunities for people with disabilities and enabling people to work from home are examples of making better use of the labour potential in The Netherlands[89].

To efficiently grow the impact of all actions on talent, more attention needs to be given to the upscaling of successful initiatives. Many great examples don't reach their full potential because their owner does not have a scaling goal. One of the tasks for us all it to identify these initiatives and support their scaling up.

3.2.2 Facilitate potential career switchers

We help security employers to fill their vacancies by tapping into the unused labour potential, not only the diverse group mentioned above, but also potential candidates with the right skills but without the right educational background, such as lateral entrants.

Proposed actions:

Continue current platforms and improve content and reach:
- to identify the need to revisit the Career Navigator[90] in view of the structure of the new European Cyber Security Framework (ECSF) and expand toward side-entrants identified by pr-edict.nl[91];
- to update the content of cybersecuritywerkt.nl ('Cybersecurity works') continuously, increase the findability of the platform and actively promote the platform among potential career switchers, job seekers, security employers including mobility centres of employing organisations, job coaches, career coaches and employment agencies (such as UWV Werkbedrijf).

Action described in detail: Revisit Career Navigator

The platform securitytalent.nl gives access to the Career Navigator[92], which is based on the Radar Safety & Security Occupations. The Career Navigator is a dynamic, intuitive, and interactive tool for those who work in the security domain and think of moving to another job within the same domain and for those who work in another domain and consider a career switch to a job in the security domain. The navigator gives insight into and overview of career opportunities by visualising the possible career pathways, job profiles, job openings and supporting education. 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, enabling the transition with the right training or education.

Action described in detail: Update platform 'Cybersecurity works'

In 2021, Security Delta launched the new platform 'Cybersecurity works' (available only in the Dutch language[93]). The platform focuses on people working in other sectors who are interested in cybersecurity jobs (potential side-entrants) and people who want or need to extend their current roles and responsibilities with cybersecurity-related tasks (job enrichment). The platform is designed to be easily accessible, attractive, inviting, appealing and informative.

The goal of the Career Navigator and the 'Cybersecurity works' platform is to attract more talent for professions in the digital security domain. To get more students and potential career-switchers (lateral or side-entrants) to choose the right development path towards an 'in demand' security position, generic factors in the selection process are information about education and career, influencers like parents, peers and educators, intrinsic motivators (interests, capabilities, ambitions) and external factors (job reputation, pay levels, development opportunities). There is still a big group first year leavers in higher education and vocational level students that do not finish 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.

3.3 Innovative learning strategies in security

By boosting innovative learning strategies in security and taking a different perspective on Education and Security, we diversify learning to attract and maintain more talent. At the same time, we might have to rethink the work we do and why and to what extend we do it.

3.3.1 Continue competence development

In section 2.4 we discuss the general trends in education and training, formal and non-formal education in the security domain, differences in education between cybersecurity and broader security; and the type of personality, skills and knowledge required from security professionals. We highlight innovative learning strategies, the power of knowledge sharing, the rise of modular education and touched upon essential skills for security professionals.

With respect to modular education and the development of broader security-related technical and non-technical skills, it would be good to investigate further (a) which type of skills are required most, now and in the future - given the expected growing needs for such skills; (b) which modules are needed, now and in the future; (c) how to measure the needs; and (d) how to structure and develop the modules over time: short term versus long term. And support and realise those that are viable.

Proposed actions:
- Continue the sharing of knowledge and innovation in the field of security on platforms like Security Insight (for example: information on the introduction and impact of NIS 2);
- Organise the International Cyber Security Summer School and National Cyber Security Summerschool, involving multiple partners from the ecosystem (annually in the month of August);
- Stimulate the development of Learning Communities where Life-Long Learning can take place and make them as effective as possible.
- Develop sector specific training on cybersecurity, such as in the installation sector[94], for SME's[95] and in horticulture[96].
- Explore the need, realise and grow education and training programmes (modularly available preferably) in the following fields:
  - Digital Security bachelor (Utrecht University of Applied Sciences)
  - Cyber Security and Cyber Governance bachelor in Dutch for 500 students/year (University Leiden)
  - AI & Security learning community (Avans Hogeschool with CVD)
  - National Introduction Course Cybersecurity (IT Verband Zuid Holland, Katapult)
  - Modular bachelor and professional master cyber engineering, associate degree Cybersecurity (The Hague University of Applied Sciences)
  - Digital Forensics master (Leiden University of Applied Sciences)
  - Strengthen cybersecurity education in The Hague (TU Delft)
  - Grow Make IT Work and WE-IT reschooling offers (Make IT Work, WE-IT)

[88] http://www.techgrounds.nl
[89] Social and Cultural Planning Office (SCP, 2022). Labour market mapped - employers: a long-term survey among employers
[90] https://securitytalent.nl/career/career-navigator-introduction
[91] https://pr-edict.nl/overstapberoepen
[92] Career Navigator on securitytalent.nl, HSD, 2020, https://securitytalent.nl/career/career-navigator-introduction
[93] https://cybersecuritywerkt.nl, HSD, 2021
[94] https://www.digitaltrustcenter.nl/samenwerkingsverband/cyberweerbaarheid-installatiebranche
[95] https://securitydelta.nl/nl/nieuws/interviews/it-verband-zuid-holland-submits-17m-application-national-growth-fund-for-security-talent
[96] https://greenportwestholland.nl/katapult-aanvraag-door-greenport-horti-campus/ and their Horti Academy.

- Cyber Education modules (University of Amsterdam)
- Master Digital Security (University of applied sciences Utrecht)
- Vocational level cyber education (ROC Mondriaan, mboRijnland)
- Social skills development, introduction programme for international talent (InnovationQuarter)
- Safety & Security course at mbo-4 level with a cybersecurity line (ROC Aventus)
- Tilburg University Professional Learning Advanced Program Cyber Security and Governance (with contributions from: NCSC, DNB, TU Delft, Microsoft, Fox-IT and CISOs ASML, Philips and Signify)

3.3.2 Promote helicopter vision and thinking in security education

In Chapter 2 we also address the topic security in conjunction with adjacent topics such as risk management, business continuity, crisis management, governance, and leadership - and noted that these topics tend to be underexposed in traditional security education. The Capstone programme is a collaboration of the technical universities in the Netherlands where we help implement a talent programme for TU students in which they do internships at security companies. This talent programme includes business and people skills (entrepreneurial skills, business development, strategy and risk, business continuity, interpreting technological developments, leadership skills, etc.). The role of disciplines like law, international relations, governance and ethics is growing in digital security.

Proposed actions:

- Explore the feasibility of expanding entrepreneurial skills programmes for security professionals and arrange funding for training, reskilling and upskilling talent;
- In collaboration with educational institutions and employers, promote the attention for and inclusion of security in a wider context – leadership, entrepreneurship, business continuity, risk management, governance – in formal and non-formal education

3.4 A common competence language for security

By tuning and implementing a common competence language for most tasks in the broader security field, connecting peoples' competences to tasks (Work) and business needs (Security) will improve matching and grow the talent pool. It will also help set requirements for individuals and education.

3.4.1 Use e-CF and ECSF for safety & security competences framework

We would welcome the development of a common competence language for the broader security domain, similar to the setup of the e-CF and ECSF. Such a competence framework would dig deeper than the current profiles of the Radar Safety & Security Occupations.
In line with the ECSF, a common competence language for the profiles and roles on the radar, or at least a meaningful selection of such profiles, would make it possible to:

- **identify** shortages relating not only to profiles and roles, but also to skills, knowledge, e-competences of e-CF;
- **analyse** the need for security professionals in an organisation: What skills and knowledge is needed? The hiring organisation could set priorities and choose the competencies and tailor the profile that suits best and use the profile in the job opening; and
- **define** needs, career paths, training itineraries for the stakeholders involved (employing organisations, educational institutions, individual professionals, and policy makers) and for external communication purposes - the bigger picture input and output including primary and secondary education, the unemployed, potential carrier switchers, the topics upskilling, reskilling, and closing the gender gap.

Proposed actions:

- Develop a common competence language for occupations within the broader security domain, along the lines of the structure of the e-CF and the new ECSF.

3.5 Keep track of developments and needs

Monitor developments in security and society that have an impact on human capital in security to have a coherent and more continuous input for governance, policy making and investing in new interventions.

3.5.1 Identify relevant developments in security and society

In Chapter 2 we describe various trends and developments that have an impact on the security domain: developments on the labour market, social trends, technological developments, regulatory tightening, and other societal developments. The paragraphs above (*3.2 to 3.4*) cover a great deal of these trends and developments. This paragraph forms a wrap-up of other developments that have not been explicitly addressed so far.

Proposed actions:

- Continue monitoring relevant developments on the labour market, amongst other things by statistic research and trend analysis. This can be done for a region, a sector or an association to better insights and specify the demand side. For example, VNG will conduct a market analysis of the labour market issues in the field of digital security for municipalities. By providing insight into exactly what the issue looks like, municipalities can then focus more specifically on possible solutions;
- Continue with the HSD-powered platform security-talent.nl; by unlocking vacancies and training in the security domain, we offer partners a platform to talent and increase the number of visitors to the site through online campaigns and other marketing efforts;
- Support automation programmes for security tasks to limit the human capital need. This can be done by regular automation, AI-support and Robotic Process Automation (RPA);
- Continue with providing relevant content on different platforms in the form of articles, an up-to-date offer of vacancies and training courses and sharing insights with employers and policymakers;
- Engage and collaborate with provinces, for instance the Province South Holland/ Economic Board South-Holland on their Human Capital Akkoord South-Holland, amongst other through WE-IT and the International talent programme, and together with Innovation Quarter.

In Chapter 4, the contents of the five connected perspectives of Chapter 2 – Talent, Education, Work, Security and Society – and the proposed actions under each perspective will essentially be interwoven in order to provide a basis to highlight the bottlenecks, target audiences and interventions. Chapter 4 is specifically set-up to provide a structured overview of which intervention is applicable to what target audience to address a particular bottleneck.

4. Intervention matrix

In the previous chapters several human capital bottlenecks came up, talent groups (*paragraph 2.2.3*) and suggested interventions were identified (*throughout Chapter 3*). The matrix below gives an overview of interventions that may help overcome the bottlenecks and affect target audiences of this agenda. The bottlenecks give another perspective on the issues previously addressed, they help clustering interventions, and are described in paragraph 4.1.
The connections that are made between the interventions, bottlenecks and target audiences are based on the current contents of the interventions. Some interventions can potentially be applied to more target audiences or contribute to overcoming more than one bottleneck. The rationale behind the interventions (*their link to the key findings from Chapter 2*) is presented in Appendix 4 – Matrix of interventions and key findings.

The matrix below helps to identify what is currently being done to tackle issues in the security labour market and clarifies which areas are addressed with more urgency than others. A description of the interventions is included in paragraph 4.2.

bottlenecks

target audience \ interventions	**A.** Talent shortage	**B.** Unattractive field	**C.** Unattractive jobs	**D.** No career perspective	**E.** Limited investment	**F.** Lack of understanding
Primary & secundary education	**9.** Connection events	**9.** Connection events **23.** Hackshield	**9.** Connection events	**9.** Connection events **23.** Hackshield		
Vocational education (mbo)	**1.** Use of skills/ competences **2.** Skills dashboard **3.** Unique learning experiences **4.** Increase modular offerings & cohesion **6.** Cyberwerf 2.0 **9.** Connection events **15.** Associate degrees **18.** Promotion of security work	**3.** Unique learning experiences **9.** Connection events **16.** Online knowledge platforms **18.** Promotion of security work	**9.** Connection events **16.** Online knowledge platforms **18.** Promotion of security work	**9.** Connection events **12.** Accessible labour & education market	**12.** Accessible labour & education market	**1.** Use of skills/ competences **2.** Skills dashboard **4.** Increase modular offerings & cohesion **12.** Accessible labour & education market **14.** Commercial certificates **15.** Associate degrees **19.** Common competence language in security
Higher education (hbo + wo)	**1.** Use of skills/ competences **2.** Skills dashboard **3.** Unique learning experiences **4.** Increase modular offerings & cohesion **9.** Connection events **15.** Associate degrees **17.** Development specific security education **18.** Promotion of security work **24.** Entrepreneurial Capstone programme **25.** Development of public professionals	**3.** Unique learning experiences **9.** Connection events **16.** Online knowledge platforms **18.** Promotion of security work	**9.** Connection events **16.** Online knowledge platforms **18.** Promotion of security work **25.** Development of public professionals	**9.** Connection events **12.** Accessible labour & education market **24.** Entrepreneurial Capstone programme	**12.** Accessible labour & education market **17.** Development specific security education	**1.** Use of skills/ competences **2.** Skills dashboard **4.** Increase modular offerings & cohesion **12.** Accessible labour & education market **14.** Commercial certificates **15.** Associate degrees **17.** Development specific security education **19.** Common competence language in security

bottlenecks

target audience

	A. Talent shortage	B. Unattractive field	C. Unattractive jobs	D. No career perspective	E. Limited investment	F. Lack of understanding
Side entrants & Lateral entrants	1. Use of skills/ competences 2. Skills dashboard 3. Unique learning experiences 4. Increase modular offerings & cohesion 5. Reschooling / retraining courses 9. Connection events 13. Cybersecurity works 18. Promotion of security work	3. Unique learning experiences 9. Connection events 16. Online knowledge platforms 18. Promotion of security work	9. Connection events 16. Online knowledge platforms 18. Promotion of security work	7. One-on-one mentoring / job coaching 9. Connection events	5. Reschooling / retraining courses	1. Use of skills/ competences 2. Skills dashboard 4. Increase modular offerings & cohesion 14. Commercial certificates 19. Common competence language in security
Untapped labour potential	1. Use of skills/ competences 2. Skills dashboard 3. Unique learning experiences 8. Tailor-made jobs 11. Attract more diverse workforce 18. Promotion of security work 21. Support HR	3. Unique learning experiences 11. Attract more diverse workforce 16. Online knowledge platforms 18. Promotion of security work	11. Attract more diverse workforce 16. Online knowledge platforms 18. Promotion of security work	7. One-on-one mentoring / job coaching 11. Attract more diverse workforce		1. Use of skills/ competences 2. Skills dashboard 19. Common competence language in security
International talent	3. Unique learning experiences 9. Connection events 18. Promotion of security work	3. Unique learning experiences 9. Connection events 16. Online knowledge platforms 18. Promotion of security work	9. Connection events 16. Online knowledge platforms 18. Promotion of security work	9. Connection events		19. Common competence language in security
Working people / workers	1. Use of skills/ competences 2. Skills dashboard 3. Unique learning experiences 5. Reschooling / retraining courses 21. Support HR	3. Unique learning experiences 10. Reshaping working conditions 16. Online knowledge platforms 22. Effective learning communities for security	10. Reshaping working conditions 16. Online knowledge platforms	7. One-on-one mentoring / job coaching 12. Accessible labour & education market	5. Reschooling / retraining courses 12. Accessible labour & education market 20. Regional and local agenda setting 22. Effective learning communities for security	1. Use of 1. Use of skills/ competences 2. Skills dashboard 12. Accessible labour & education market 14. Commercial certificates 19. Common competence language in security
Working people / workers with a security profession	1. Use of skills/ competences 2. Skills dashboard 3. Unique learning experiences 21. Support HR 25. Development of public professionals	3. Unique learning experiences 10. Reshaping working conditions 16. Online knowledge platforms 22. Effective learning communities for security	10. Reshaping working conditions 16. Online knowledge platforms	7. One-on-one mentoring / job coaching 12. Accessible labour & education market 25. Development of public professionals	12. Accessible labour & education market 20. Regional and local agenda setting 22. Effective learning communities for security	1. Use of skills/ competences 2. Skills dashboard 12. Accessible labour & education market 14. Commercial certificates 19. Common competence language in security

interventions

4.1 Bottlenecks

Bottlenecks give another perspective on the issues addressed throughout this agenda; they help clustering interventions. There are other bottlenecks and those formulated here are not underpinned with studies but are recognisable themes withing human capital for security. Some more generic actions that support the whole agenda are not placed in this frame, this is no indication of importance.

A. Talent shortage

Currently talent- and staff shortages dominate the Dutch labour market, including the security sector. People working in security occupations and security-related functions generally have a higher level of education. They are middle-aged or older, which calls for attracting young talent and monitoring of the overall age structure of the workforce. However, current vacancies are more targeted against seniors than juniors, making it hard for young talent to obtain security-related jobs.

Furthermore, labour market supply and demand do not match well. Employers sometimes make unrealistically high demands on candidates and are then surprised that there is no one to get. Employees also sometimes make high demands: at least market-based salary, good working conditions, tailor-made work, determine their own working hours and location, attractive career prospects, etc. This mismatch is one of the causes of the large group of unused labour potential.

B. Unattractive field

The security sector has become unattractive over the years. There are, amongst other obstacles, problems with an ageing workforce (e.g. within the police), a decrease in the number of students in intermediate vocational / practical education, (sometimes) a difficult work culture and a diversity problem. All these factors lead to the security field becoming increasingly unattractive to new talent or other individuals.

C. Unattractive jobs

There are several factors that have led to some jobs being unattractive in the security sector. For example, high working pressure, weak organisational embedding, limited resources, unclear roles and responsibilities, monotonous jobs, and a lack of recognition for work achievements. All these factors lead to lower quality jobs and less motivated workers.

D. No career perspective

Some people that are working in the field of security leave the field due to a lack of a career plan or career perspective. Within their employment there are no possibilities to be further educated or move up the ranks to a higher position. Furthermore, no tool or guidance is offered to help these individuals with finding the next step in their security-related career. Therefore, there is a need to scale up skills-based and career-path tools.

E. Limited investment in development, retraining and upskilling

There are limited investments being made in the development, retraining, and upskilling of currently employed individuals in the security sector or individuals that have the intention of obtaining a security-related profession. There is a lack of resources available to address this issue.

F. Lack of understanding

Currently, there is a lack of structure and oversight in formal and non-formal education in the security domain. There is a huge quantity of education, training, and courses. People can no longer see the wood for the trees. This is a problem. It hinders people from making the right choice from the offerings in their personal situation.

Furthermore, there is a difficult connection between courses, training, and education, and the requirements (skills, experience) of jobs. On the one hand, employers are unclear with regards to job descriptions and what people they specifically want. On the other hand, solution providers & educators do not match the demand of employers. This all leads to a lack of understanding between educators and employers.

4.2 Interventions

1. Use of competences/skills instead of formal education

To address the lack of understanding between employers and educators, there is a need to focus on the use of competences, skills and potential instead of on someone's previously followed formal education. The introduction of a generally agreed-upon skills passport helps reduce the lack of understanding between employers and educators. The skills passport includes the skills and competences of an individual, which can respectively be matched with the needs of an employer (skills-based matching).

2. Skills dashboards
There is an increasing need to provide insight into what types of skills are in demand in the security sector. It is important to map out the types of skills in order to adjust and provide the correct types of trainings, courses and other forms of education. Skills dashboards, such as the 'dashboard skills' of the UWV and SBB, and the 'house of skills' of the AEB, are used to provide insight into the skills demand and larger trends and developments in the labour market.

3. Unique learning experiences
In order to make potential new talent and other individuals enthusiastic and interested in security-related professions, unique learning experiences can be utilized. Bootcamps, hackathons, datathons and other similar events provide insight into the workings of security-related professions. For example, the annually organised International Cyber Security Summer School provides the opportunity for young professionals, PhD-students and master-students to broaden their knowledge in the field of cybersecurity, where the National Cyber Security Summerschool attracts talents that have not yet chosen for this field to grow the talent pool. Another example is the annual Challenge-the-cyber[97]. Challenge-the-cyber organises cybersecurity events for scholars and students. The annual Challenge the Cyber CTF, the Cyberbootcamp and the mission to the European Cybersecurity Challenge are the main pillars, and training and networking activities.

4. Increase modular offerings & cohesion
It is important to increase the cohesion between modular education courses of different education providers. Modular cohesion also plays an important part to meet the demands of employers. An example of more cohesion is the initiative from IT Campus Rotterdam:
Rotterdam wants to work from the incidental training places (Hackatons) towards structural learning lines and training with their partners. IT Campus Rotterdam will direct this so that connections can arise across the boundaries of institutions.

Furthermore, there is a need to explore new education programmes in the fields of AI, forensics, cyber resilience, and human skills. For example, the Informatics Institute of the University of Amsterdam started focusing on developing short IT masterclasses for professionals, including (cyber)security masterclasses. These masterclasses are all based on the fundamental scientific research of the Institute and the strong industrial experience.

5. Reschooling/retraining courses
Currently there are various reschooling and retraining courses available for side entrants and lateral entrants to become a professional in the security sector. Highlighting and promoting such courses is important to close the talent gap. Also, traineeships can be made part of this where new talent are supported to learn and develop quickly during their first period at an employer. Examples of reschooling and retraining platforms and programs are:
- *Techgrounds.* The unique IT orientation programme for career switchers with or without any background in IT; during the Pathways programme, potential candidates match their skills, talents, and past experiences to either upskill or start a successful career in IT.
- *TekkieWorden*. This platform provides insight in more than 400 IT-studies, courses and trainings, destined for various target audiences.
- *Make IT Work!* MITW provides the possibility for individuals with a hbo or wo background to be retrained for an IT-related job. Participants do not need any initial experience with IT to participate in the programme.

6. Cyberwerf 2.0
Cyberwerf is a programme that started at the Security Field Lab, with the support of the Economic Board of The Hague, the Municipality of The Hague and ROC Mondriaan. This programme allows vocational level (mbo) students to work as SME cybersecurity consultants. The set-up, model and results of Cyberwerf are promising. Therefore, this intervention focuses on exploring a further continuance of the programme (Cyberwerf 2.0).

7. One-on-one mentoring / job coaching
One-on-one mentoring and job coaching are two ways to address the limited career perspective bottleneck within the security sector. One-on-one mentoring focuses on intensive guidance by, for example the UWV and 'werkgeversservicepunten' of municipalities, to provide opportunities for unemployed individuals to enter or re-enter the security labour market. Job coaching focuses on individuals that already engage in a parttime or fulltime position within the security sector. Job coaching is utilized to provide career perspective and possible opportunities for individual development. In terms of providing career perspective, individuals can for example utilize the Career Navigator embedded within Security Talent to orientate themselves on future job opportunities. Other forms of job coaching focus on the further development of relevant knowledge and expertise by engaging in for example peer learning and expert groups (such as a peer learning group of CISO's).

8. Tailor-made jobs
Tailor-made jobs and standardised jobs are jobs for employees who are unable or unwilling to work full time at a high pace due to, for example chronic illness, disability, age (say 55-plus) or personal circumstances. These types of jobs are situated in a protected work environment and usually provided by governmental bodies, such as municipalities. Examples of tailor-made jobs are:
- *Helpdesk personnel / call-centre personnel*. Individuals can be trained and coached in order to function as a first point of contact for organisations that endure problems with their IT-infrastructure.
- *Installer.* Individuals can be trained to be installers of physical IT/IoT applications. Installing camera's, sun panels, digital doorbells, routers and sensors are example of such physical applications.
- *Wi-Fi-network controller.* Standardized tests of WiFi networks are usually performed by individuals with a specialised IT-background. However, with a standardized plan, individuals with lower or no qualifications are able to perform WiFi network tests as well.

9. Connection events
Connection events encompass a wide range of events to attract and stimulate new talent for the security sector. A few examples:
- *Open days* are utilized within secondary education, mbo, hbo and wo in order to provide insights into security-related education.
- *Career markets* are held on mbo, hbo and wo to affiliate new talent with possible job opportunities within the field.
- *Guest-speakers* are utilized to for example affiliate children and young adults within primary and secondary education with the security domain, but are also utilized within mbo, hbo and wo to provide enthusiastic lectures about a security-related profession or topic.
- *Match making* is a way to facilitate the demand from organisations and supply side so there is a better match between them. For example the project 'Fresh look at the labor shortage in municipalities – (Frisse blik op de arbeidskrapte bij gemeenten)' the VNG focuses on connecting talent with an affinity with digital security at universities of applied sciences and universities with municipalities.

10. Reshaping working conditions
Given the huge tightness in the labour market, it is important for employers to know how to retain their employees and prevent people from dropping out. Therefore, reshaping working conditions within an organisation can significantly help with retaining current employees and provide possibilities to attract more talent. Reducing work pressure, automate mundane tasks, offering education and training, providing opportunities for people with disabilities, enabling flexible work arrangements[98], showing employees that they are valued[99] are some examples of reshaping working conditions that make both the security field and jobs more attractive.

11. Attract a more diverse workforce
As the influx of women in STEM-education is significantly lower than the influx of men, it is important to address this issue to grow a more diverse workforce in digital security. There are several ways to attract a more diverse workforce within the security sector, thereby including more women and underrepresented groups:
- *Enhancing visibility* of women and underrepresented groups at work in security via the two talent platforms powered by HSD (securitytalent.nl and cybersecuritywerkt.nl);
- *Sharing best practices* on attracting and retaining women and underrepresented groups (role models, network opportunities, safe and pleasant work environment, work-life balance choices, inclusive performance appraisals);
- *Enlarging the pool of potential security talent* by coaching, mentoring, and supporting women and under-represented groups (for instance refugees, such as Accenture does[100]) who are interested to work in security.
- *Provide perspective and guidance to (ICT) talents who are on the sidelines.* For example, social enterprise ITvitae

[97] https://challengethecyber.nl initiative of the National Cyber Security Centre and dcypher

[98] https://www.weforum.org/agenda/2023/05/the-cybersecurity-skills-gap-is-a-real-threat-heres-how-to-address-it
[99] https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[100] https://refugeetalenthub.com

was founded in 2013 with a social purpose: to provide perspective and guidance to ICT talents who are on the sidelines due to autism or giftedness and help them pursue a career as ICT professionals through education, mediation, and guidance provided by experienced ICT professionals and job coaches.

- *More visibility of initiatives for underrepresented groups by campaigning.* For example, ITvitae and the Driessen Foundation launched a campaign called “More Women in IT,” where women have the opportunity to receive a scholarship to study at ITvitae.
- *Provide training programmes for women.* Train women to be more aware of the possibilities in tech and create opportunities for women to take on a technical role such as the Equals Academy[101].

12. Accessible labour & education market

It is of upmost important that the security labour and education market is accessible to all interested parties. In order to achieve the desired accessibility, various options can be implemented. For example, by providing fitting job descriptions, (re)structuring of courses, trainings and vacancies, and providing accurate labour market analyses, the accessibility to the security labour and education market can be improved. Security Talent functions as a platform that brings together all of these available options in a structured overview. Therefore, it is important to further develop Security Talent in various ways:

- Continue the HSD-powered platform securitytalent.nl by unlocking vacancies and training in the security domain, we offer partners a platform to talent and increase the number of visitors to the site through online campaigns and other marketing efforts;
- Continue with providing relevant content on securitytalent.nl in the form of articles, an up-to-date offer of vacancies and training courses and sharing insights with employers and policymakers;
- Continue with data analysis of the vacancies/ job openings and the training courses posted on securitytalent.nl;

13. Cybersecurity works platform

The platform cybersecuritywerkt.nl (in Dutch) can be utilized to attract side- and lateral entrants that are interested in retraining and reschooling for jobs within the security sector. Therefore, it is important to:

- Update the content of cybersecuritywerkt continuously, increase the findability of the platform and actively promote the platform among potential career switchers, job seekers, security employers including mobility centres of employing organisations, job coaches, career coaches and employment agencies (such as UWV Werkbedrijf);
- Continue the HSD-powered platform cybersecurity-werkt.nl to attract lateral entrants to the cybersecurity domain, by connecting other sectors and employers, organising or supporting orientation meetings for career switchers and cooperation with other retraining initiatives.

14. Commercial certificates

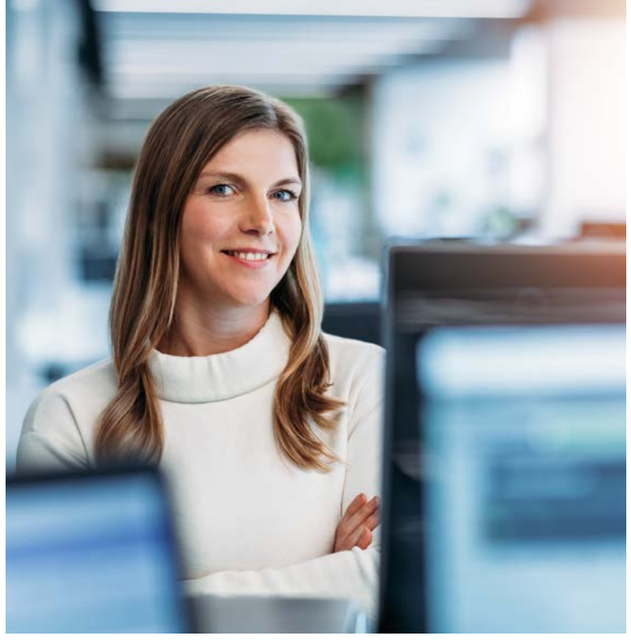
Commercial certificates function as an addition to a regular training, course, bachelor or master degree. It allows individuals to become familiar with certain specialities that are necessary for particular (niche) jobs, such as CISM and CISA certifications. Commercial certificates are important to incorporate within the interventions of this HCA, because these certificates have the ability to quickly adapt to the demand of the security labour market. If new demand arises for certain certifications, commercial certificate providers have the ability to develop new courses/trainings.

15. Associate degrees

Within the transition of security-related vocational education (mbo) to higher education (hbo) a large discrepancy can be seen in terms of difficulty, which leads to mbo-students not being able to transition to hbo. In order to address this issue, associate degrees can be incorporated for security-related hbo-education. An associate degree is a course/training of two years of which the difficulty level lies between mbo level 4 and hbo, making it easier for mbo-students to transition to higher education. Within the curriculum of an associate degree there usually is room to gain practical experience in the field, thereby closing the gap between education and the labour market.

The Associate degree is not only a suitable course for young adults for whom the step to a full hbo bachelor’s degree is too great, but also for adult re-skillers or re-schoolers because of the limited duration and the civil effect of the course. Consultation with the professional field is necessary to increase awareness of the Associate degree and to have this program included in the job and salary houses.

[101] https://we-itwerkt.nl/onze-programmas/equals-academy



16. Online knowledge platforms

Online knowledge platforms have the ability of providing an overview of knowledge and information regarding security-related topics. Easily accessible structured information is important to provide in order to reach a wide variety of target audiences that are interested in the security sector. A platform, such as Security Insight, shares knowledge of innovation in the field of security on a daily basis (for example: information on the introduction and impact of NIS 2), thereby providing new avenues for people to gain access to the security sector.

17. Development specific security education

Currently, there are multiple general security-related courses, trainings and long-term forms of education, such as the hbo-bachelor Safety and Security Management Studies and wo-bachelor Computer Science. Building on these courses/trainings, the feasibility of developing specific security education comes to the front. For example, exploring the feasibility of setting up an entrepreneurial skills programme for security professionals provides space for more specialised trained security personnel. In paragraph 3.3.1 there is a longer list of specific security education to develop and support. It is important to keep exploring and developing new specific security education according to the demand of the security labour market.

18. Promotion of security work

It is important to, for example in collaboration with educational institutions/HSD partners, promote the attention for and inclusion of security in a wider context - leadership, entrepreneurship, business continuity, risk management, governance - in formal and non-formal education. The promotion of security work focuses on non-professionals that have the potential to become a security professional. Through knowledge sessions, guest lectures and other promotional advertisement, the ins and outs of security-related professions in the security sector are communicated to the target audience. This may include incorporating cybersecurity or risk management in technical- and business administration, accountancy, law studies. But also strengthening cybersecurity education in IT-studies. Realizing lateral influx is becoming increasingly important. This means that organisations will have to set up attractive processes together with the educational and knowledge institutes that focus on recruiting and training lateral entrants, but also on removing any (financial) barriers.

19. Common competence language in security

Exploring the feasibility of developing a common competency language for occupations within the broader security domain has the potential to provide clearer organisation and better overview of available jobs. A common competence language allows for more detailed and continuous monitoring of the demand and supply of the security labour market. The ENISA Skills framework CS (ECSF) can function as a starting point from which the common competence language can be further developed.

20. Regional and local agenda setting

It is essential that the national ambitions regarding the security labour market also resonate with regional and local agendas. Making sure that the national, regional and local ambitions are in sync with one another provides more leeway for the implementation of proposed interventions and action lines. For example, by engaging and collaborating with the Province South-Holland and the Economic Board South-Holland on their Human Capital Agreement South Holland, national ambitions are translated into regional and local investments. Other important investment agendas are for example: WE-IT, ‘internationaliseringsprogramma Cybersecurity’ (InnovationQuarter), Human Capital Agenda The Hague and the agenda of the IT Campus Rotterdam.

21. Support HR

HR plays a crucial role in the recruitment and retainment of new and current employees. Therefore, providing various types of support to HR can be crucial to the further development of an organisation. There are multiple ways to support HR professionals, amongst others to organise a series of knowledge sharing and networking events for recruitment/HR around topical issues in the field of talent,

work and security, in order to: attract younger generations; attract a more diverse workforce; attract potential talent, currently part of the untapped labour potential; explore job engineering/ job enrichment in security; and share insights of HR as to how to support the development of the CISO role within security organisations.

22. Effective learning communities for security
Learning communities come in all shapes and sizes: living labs (such as in Scheveningen and the Amsterdam ArenA), round tables, peer-learning sessions, HSD cafés and many more. The essence of a learning community is to utilize the expertise of others in order to personally become more effective and knowledgeable in certain areas. Since many different forms and types of learning communities exist, the question arises how to properly organise and structure these communities in the best way possible. Exploring the feasibility of (re)structuring and creating better connections between learning communities as well is improving the community guidance itself, can lead to more effective learning communities for the security sector.

23. Hackshield
Hackshield is a project where children between the ages of eight and twelve are stimulated to learn more about cybercrime. By utilizing a 'game-teaching method', where children pretend to be cyberagents, various questions and puzzles are solved that are focused on cybersecurity. Due to the increasing digitalisation of our society, it is important to teach children how to behave and what they can expect within the digital domain. Hackshield provides both opportunities to stimulate and enthuse children for the security sector and teaches them the important dangers of the digital domain. The project is applicable on a national scale and focuses mainly on primary and secondary education.

24. Entrepreneurial Capstone programme
Helping implement a talent programme for technical university students, in which they do internships at cybersecurity companies and train their entrepreneurial skills. It grows the number of start-ups and career perspective of cybersecurity talent.

25. Development of public professionals
Specifically for the development of professionals in the public sector, also in digitalisation, security, cybersecurity, privacy and other relevant topics for this agenda, several training and development initiatives are taken, and high-quality content is made available. This often done in collaboration with other government partners, educational institutes and businesses. Great initiatives include:

- I-Vakmanschap programme for National Government[102], which includes I-Partnerschap (collaboration with educational institutes), I-Doctoraat (PhD programme), I-Stage and I-Traineeship (internship and traineeship programme), LOC Platform (learning and development platform) and detailed descriptions of development paths also in cybersecurity and inspired on the e-CF.
- The Centre for Information Security and Privacy Protection is a public-private network organisation that shares knowledge with and between government professionals with support of industry. Tools, guidelines, games, lectures and an active community support learning about awareness, guidelines, technology, privacy protection, secure software development and more.
- The VNG (municipalities) and police set up a joint programme for leadership in the digital society. Next to this, they plan to conduct a market analysis of the labour market issues in the field of digital security for municipalities and VNG will start in 2023 with matchmaking interns on safety, security and privacy.

The further development and rollout of these initiatives grows professionalism, development and attractiveness of working for governmental organisations.

4.3 Next steps

Several of the interventions mentioned in paragraph 4.2 are already developed or active. Some are waiting for initiative and/or funding; others have a limited scale or target group and with the right support could contribute to further growth and impact of the talent pool. Coherence, coordination, and execution are currently more incidental and mostly unfunded, this agenda is a step up in this respect and needs to be secured. Local, regional, and sectoral translations need to be made and invested in to support and realise the mentioned ambitions. Next to the visibility of this agenda is the incorporation of relevant actions and interventions that are not yet included to strengthen the execution. A joint financial and action plan based on this agenda by the partners mentioned in Chapter 1 and (some of) the supporters in is a necessary next step. This agenda is the basis for future collaboration with dcypher, Topsector ICT, the Ministry of Economic Affairs and the broader national government on the topic. Goal is to connect to developing national policies to maximize execution power and coherence.

[102] https://www.rijksorganisatieodi.nl

Appendix 1 – Consulted organisations

The writers worked and talked with many organisations that delivered valuable input for the content of this Human Capital Agenda Digital Security. In particular the work and inputs of the following organisations have supported the drafting of this document or proposed interventions (in alphabetical order):

- Accenture
- Amsterdam University of Applied Sciences
- Awareways
- AXite Security Tools
- Belastingdienst
- BOEM Consultants BV
- Booz Allen Hamilton
- BTG
- Cegeka
- Centrum voor Veiligheid en Digitalisering (CVD)
- CFLW Cyber Strategies
- Chapter8
- City of Amsterdam
- City of Apeldoorn
- City of The Hague
- Connect2Trust
- Crisisplan BV
- Cyberveilig Nederland (CVNL)
- DIVD Academy
- DongIT
- Dutch Innovation Factory
- Economic Board Zuid-Holland (EBZ), Taskforce Human Capital
- ECP
- Guardian360
- Greenport West-Holland
- HBO-i
- Hudson Cybertec
- IDentity Next
- InnovationQuarter
- ISACA
- IT Campus Rotterdam
- ITvitae
- KPN Security
- Leiden University
- Leiden University of Applied Sciences
- LOI
- MboRijnland
- NIPV
- NLwerktaanwerk
- NTI
- Pandora Intelligence
- Police Academy
- Province of Gelderland
- Province of Overijssel
- Province of South Holland
- ROC Aventus
- ROC Mondriaan
- RONT Management Consultants
- Saxion University of Applied Sciences
- SECO-Institute
- Secura
- Security Academy
- Security Coaches
- Security Delta (HSD)
- Security Management StudentenPlatform (SMSP)
- Signpost Six BV
- Stichting Alumni Integrale Veiligheid (AIV)
- The Association of Netherlands Municipalities (VNG)
- The Hague University of Applied Sciences (THUAS)
- ThreadStone Cyber Security B.V.
- Tilburg University
- TNO
- University of Amsterdam
- University of Applied Sciences Utrecht
- University of Twente
- VNO-NCW West
- VNO-NCW
- WE-IT
- Work in Rotterdam-The Hague

Appendix 2 – Results HCA Security 2019-2022

Since 2019 Security Delta (HSD) executed the Human Capital Agenda Security 2019 – 2022, which we developed in close collaboration with 40+ partners. The goal of the agenda was to tackle the discrepancies in the labour market by improving the qualitative and quantitative match between demand and supply of security personnel. Because access to talent is a crucial prerequisite for the creation of innovative security solutions and the growth of the security sector. As part of the Human Capital programme, we have developed several projects and activities. Some highlights:

- Supporting the connection between education and labour market took shape in 122 guest lectures and company visits, 173 internships were filled through P@CT and the 4TU cybersecurity capstone entrepreneurship, and we helped in realising 5 career events where employers meet talent. Together with partners we trained 20 Human Resource professionals in cybersecurity recruitment. We helped starting 'Cyberwerf', a collaboration between several HSD partners and companies at industry park ZKD. The initiative won the Computable awards in 2019.
- Several tools were developed to support the work that stems from the Human Capital Agenda. Our securitytalent-platform has been enriched with a Career Navigator and a Dashboard of job-openings. We shared 5,427 vacancies, 612 studies per year connected to 44 job profiles. This resulted in an average of 4,112 visits per month. We launched a new platform: www.cybersecuritywerkt.nl where everyone can find out whether a switch to the cyber domain or a cybersecurity job enrichment is of interest for them and how to take the next step towards this exciting field. To educate entrepreneurs, specifically of small and medium sized enterprises, we developed ikhebcyberkracht.nl to raise awareness and action against cyberthreats.
- Together with Europol EC3, NATO's CI Agency, Leiden University, and many other HSD partners, we organised the 'International Cyber Security Summer School' three times (one was cancelled due to the COVID pandemic, one was online), hosted from The Hague. Together, 183 students and young professionals from 20+ nationalities attended lectures on the most current cybersecurity topics. They were also challenged with cases from partners to work on new solutions that make our online activities safer.
- Several other training and education activities were supported, including the P@CT-program that resulted in cyber education for 1,133 vocational level students and 31 lecturers trained in cybersecurity. Two new Master programs were developed and started (International Security and Cyber Security Engineering), three new courses (Ethical Hacking, Cyber Security Risks, IT Risk Management) and 4 new electives (3 on vocational level, 1 on pre-vocational level).
- HSD Office published 11 articles about the need for talent and labour market developments and commenced and/or co-authored 4 studies to support problem analysis, policy making and practical interventions. Topics included a broader study into the education and labour market in the security domain, possibilities and requirements for using hybrid cybersecurity teachers, and side-entrants for cybersecurity functions.
- HSD Office also joined and helped set up several regional initiatives that align with our HCA-goals such as the re-school programme We-IT (support career switchers toward IT-functions), the attraction of International Talent and Human Capital in Cybersecurity for SME's. Programs and initiatives elicited investments in the tackling the Human Capital challenges of 2.4 M€.

The highlighted results of the HCA Security 2019 – 2022 are summarised in Figure 12. Best result for the network function of HSD is the support and involvement of at least 107 organisations in realising the coordinated set of activities, their logos are shown in Figure 13. We would like to thank them for their support and great cooperation in the activities and welcome them and others to contribute to the coming years.

Figure 12: Results HCA Security 2019-2022

Figure 13: These organisations have contributed to the HCA activities the last four years.
(Some organisations have since changed their name)

Appendix 3 – Matrix of actions and key findings

Action line 3.2.1 Support HR professionals

Proposed actions	Key findings
• Attract younger generations	TALENT 1,2,3 WORK 2,3 SECURITY 1 SOCIETY 1,3
• Attract a more diverse workforce	TALENT 1,2,3 EDUCATION 2 WORK 1,2,3 SOCIETY 1,3
• Attract potential talent, currently part of the untapped labour potential	TALENT 1,2,3 EDUCATION 2,4 WORK 1,2,3 SECURITY 1 SOCIETY 1,3
• Explore job engineering/ job enrichment in security	TALENT 2 EDUCATION 1,2,3 WORK 1,2,3 SECURITY 1,2,3,4 SOCIETY 2,4

Action line 3.3.1 Continue competence development

Proposed actions	Key findings
• Continue the sharing of knowledge and innovation on platforms Security Insight	EDUCATION 1,2 WORK 1,3 SECURITY 3,4 SOCIETY 1,4
• Organise summerschools on cybersecurity (ICSSS and NCS3)	TALENT 1 EDUCATION 3 WORK 2,3 SECURITY 4 SOCIETY 1
• Stimulate development of learning communities	EDUCATION 1,2,4 SOCIETY 1,2,4
• Develop sector specific training on cyber-security	TALENT 2,3 EDUCATION 1,2,3,4 WORK 3 SECURITY 1 SOCIETY 1,2,4
• Explore the need, realise, and grow education and training programmes	TALENT 2,3 EDUCATION 1,2,3,4 WORK 2,3 SECURITY 2,3,4 SOCIETY 1,2

Action line 3.4.1 Use e-CF and ECFS for safety & security competences framework

Proposed actions	Key findings
• Develop a common competence language for occupations in the security domain	TALENT 2 EDUCATION 2,3,4 WORK 1

Action line 3.2.2 Facilitate potential career switchers

Proposed actions	Key findings
• Continue current platforms and improve content and reach: identify the need to revisit the Career Navigator in view of the structure of the new European Cyber Security Framework (ECSF) and expand toward side-entrants identified by pr-edict.nl	TALENT 2 EDUCATION 1 WORK 1,2 SECURITY 4
• Continue current platforms and improve content and reach: update the content of cybersecuritywerkt.nl continuously, increase the findability of the platform and actively promote the platform among potential career switchers, job seekers, security employers including mobility centres of employing organisations, job coaches, career coaches and employment agencies (such as UWV Werkbedrijf)	TALENT 1,2,3 EDUCATION 1,2,3,4 WORK 1,2,3 SECURITY 1,4

Action line 3.3.2 Promote helicopter vision and thinking in security education

Proposed actions	Key findings
• Explore the feasibility of expanding entrepreneurial skills programmes and funding for training, reskilling, and upskilling	TALENT 3 EDUCATION 1 WORK 3 SECURITY 2 SOCIETY 1
• Promote the attention for and the inclusion of security in a wider context (risk, formal/ informal education)	EDUCATION 1,2,4 WORK 1,3 SECURITY 1,2,4 SOCIETY 1,3

Action line 3.5.1 Identify relevant developments in security and society

Proposed actions	Key findings
• Continue monitoring relevant developments in the labour market (statistic research and trends)	TALENT 2 EDUCATION 2,3 WORK 1 SECURITY 2,3,4 SOCIETY 1,2
• Continue securitytalent platform	EDUCATION 1,3 SECURITY 1 SOCIETY 1
• Support automation programmes for security tasks (AI)	WORK 2 SECURITY 1,3 SOCIETY 1,2,3
• Continue with providing relevant content on different platforms (articles, vacancies)	TALENT 3 EDUCATION 1,2 WORK 1,3 SECURITY 1,2,3,4 SOCIETY 2,4
• Engage and collaborate with others (IQ, etc.)	WORK 2,3 SECURITY 3,4 SOCIETY 1,2

Appendix 4 – Matrix of interventions and key findings

Proposed actions	Key findings
1. Use of skills/competences instead of formal education	TALENT 2,3 EDUCATION 2,3,4 WORK 1,2,3
2. Skills dashboards	TALENT 2 WORK 1,3
3. Unique learning experiences	EDUCATION 1 WORK 1,2,3
4. Increase modular offerings & cohesion	TALENT 3 WORK 1,2
5. Reschooling/retraining courses	TALENT 3
6. Cyberwerf 2.0	TALENT 1 EDUCATION 1 WORK 2,3 SECURITY 3
7. One-on-one mentoring / job coaching	TALENT 1 EDUCATION 1 WORK 2,3
8. Tailor made jobs	TALENT 1 WORK 1,2,3 SECURITY 1,2
9. Connection events	TALENT 1 WORK 2,3
10. Reshaping working conditions	TALENT 1 WORK 3
11. Attract a more diverse workforce	TALENT 1,2,3 EDUCATION 2 WORK 1,2,3 SOCIETY 1,3
12. Accessible labour & education market	TALENT 2 EDUCATION 3 WORK 1,2,3

Proposed actions	Key findings
13. Cybersecurity works platform	TALENT 1,2,3 EDUCATION 1,2,3,4 WORK 1,2,3 SECURITY 1,4
14. Commercial certificates	EDUCATION 2 SECURITY 2,4
15. Associate degrees	EDUCATION 1,2,3,4 WORK 2
16. Online knowledge platforms	EDUCATION 1,2 WORK 1,3 SECURITY 3,4 SOCIETY 1,4
17. Development specific security education	TALENT 3 EDUCATION 1,2,3,4 SECURITY 2,4
18. Promotion of security work	TALENT 3 WORK 1,3
19. Common competence language in security	TALENT 2 EDUCATION 2,3,4 WORK 1
20. Regional and local agenda setting	WORK 2,3 SECURITY 3,4 SOCIETY 1,2
21. Support HR	TALENT 1,2 WORK 1,3
22. Effective learning communities for security	EDUCATION 1,2,4 SOCIETY 1,2,4
23. Hackshield	TALENT 1,3 EDUCATION 1
24. Entrepreneurial Capstone programme	TALENT 1,3 EDUCATION 1,2,3,4 WORK 3
25. Development of public professionals	TALENT 2,3 EDUCATION 1,3,4 WORK 1,2,3 SECURITY 1,3,4

Publication information
Human Capital Agenda Security 2023 – 2026

A publication from
Security Delta (HSD)
Wilhelmina van Pruijsenweg 104
2595 AN Den Haag
T + 31 (0)70 204 5180
Info@securitydelta.nl
www.securitydelta.nl
@HSD_NL

Centrum voor Veiligheid en Digitalisering (CVD)
Bezoekadres:
Wapenrustlaan 11
7321 DL Apeldoorn
www.cvdnederland.nl
info@cvdnederland.nl

Authors
Mark Ruijsendaal (editor), Mira van Benthem
Paula Kager, Max Kroes & Ben Kokkeler

Design
RAZA Graphic Design
(by the initial design of Studio Koelewijn Brügenwirth)

Images
iStock

Print
Drukkerij Rijser BV

HSD
securitydelta.nl

W. van Pruisenweg 104
2595 AN Den Haag
securitydelta.nl