PLATO
Platform Opleiding, Onderwijs en Organisatie B.V.
Universiteit Leiden

Arbeidsmarkt voor Cyber Security Professionals



Onderzoek in opdracht van het Wetenschappelijk Onderzoek- en Documentatie Centrum (WODC) Ministerie van veiligheid en Justitie.

December 2014

Dr. J.A. van Lakerveld
Drs. S.D. Broek
Drs. B.J. Buiskool
Drs. D.H. Grijpstra
Drs. I. Gussen
Drs. I.C.M. Tönis
Drs. C.A.J.M. Zonneveld

COLOFON

Opdrachtgever

Wetenschappelijk Onderzoek- en Documentatie Centrum (WODC)
Afdeling Externe Betrekkingen (EWB)
Ministerie van Veiligheid en Justitie
Schedeldoekshaven 131
2511 EM Den Haag

Onderzoekers

Het onderzoek is uitgevoerd door PLATO (Platform Opleiding, Onderwijs en Organisatie BV) van de Universiteit Leiden in samenwerking met Ockham IPS, Utrecht.

PLATO BV (Universiteit Leiden):
Dhr. dr. J.A. van Lakerveld (projectleider)
Mw. drs. I. Gussen
Mw. drs. I.C.M. Tönis
Mw. drs. C.A.J.M. Zonneveld

Ockham IPS:
Dhr. drs. S.D. Broek
Dhr. drs. B.J. Buiskool

Bij het onderzoek betrokken externe experts

Dhr. drs. D.H. Grijpstra, expert op het terrein van arbeidsmarktonderzoek (Panteia)
Dhr. dr. J.A. van Wilsem, expert op het terrein van internetcriminaliteit en cybersecurity-issues in de samenleving (Universiteit Leiden, Faculteit Rechtsgeleerdheid, afdeling Criminologie)

Begeleidingscommissie

Dhr. prof. dr. ir. J. van den Berg, TU Delft (voorzitter)
Mw. drs. J.R. Bax / dhr. drs. A.J. Steenbrink, Ministerie van Onderwijs, Cultuur en Wetenschap
Mw. dr. Y.K. Grift, Utrecht University School of Economics
Dhr. dr. G. Haverkamp, Wetenschappelijk Onderzoek- en Documentatiecentrum
Dhr. drs. G.D. Klein Baltink / mw. drs. E. Attema, Ministerie van Veiligheid en Justitie, NCTV
Dhr. prof. dr. B. van Lier, Centric Netherlands / Steinbeis University Berlin
Mw. drs. A.M. Vos / dhr. J.P.G. Verhagen EMSD, Ministerie van Veiligheid en Justitie, NCTV
Mw. J. van Zoggel, Stichting Cyber Security Academy The Hague

© 2014, WODC, Ministerie van Veiligheid en Justitie. Auteursrechten voorbehouden.

Voorwoord

Voor u ligt de rapportage van het onderzoek naar de arbeidsmarkt voor Cyber Security Professionals (CSP's). Zoals benadrukt in de Nationale Cybersecurity Strategie 2 (NCSS2) zijn voldoende Cyber Security Professionals nodig om optimaal gebruik te kunnen maken van de kansen die digitalisering ons biedt en om ons weerbaar te maken tegen de steeds geavanceerdere dreigingen. CSP's zijn ook hard nodig om cybersecurity-oplossingen voor de toekomst te ontwerpen en te bouwen. Een tekort aan deze professionals gaat gepaard met de nodige risico's voor (vitale) systemen die van belang zijn voor de Nederlandse economie, veiligheid en vrijheid van burgers.

Vraag en aanbod op de arbeidsmarkt voor CSP's moet in voldoende mate met elkaar in evenwicht zijn om tijdig en adequaat te kunnen reageren op kwetsbaarheden en dreigingen (ook preventief en proactief). Daarom wil de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) inzicht krijgen in de aard en omvang van een (eventueel) tekort aan deze professionals (zowel technisch dominant als niet technisch dominant) en oplossingsrichtingen identificeren om eventuele tekorten op de arbeidsmarkt op korte en middellange termijn te reduceren.

In dit kader heeft PLATO BV van de Universiteit Leiden in samenwerking met Ockham IPS een arbeidsmarktonderzoek verricht naar vraag en aanbod van Cyber Security Professionals. Dit onderzoek is uitgevoerd in opdracht van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (WODC) van het ministerie van Veiligheid en Justitie.

Voor de begeleiding van dit onderzoek was een commissie samengesteld, onder leiding van prof. dr. ir. J. van den Berg (TU Delft) waarin alle voor het onderzoek relevante domeinen vertegenwoordigd waren. Wij danken de leden van de begeleidingscommissie voor hun kritische blik, suggesties en creatieve ideeën. Hun inbreng was voor het onderzoeksteam een extra stimulans om het arbeidsmarktvraagstuk op het terrein van CSP vanuit alle relevante invalshoeken te benaderen.

Ook gaat onze dank uit naar de twee externe experts die vanaf de opzet van het onderzoek betrokken waren, drs. D.H Grijpstra (arbeidsmarktdeskundige, Panteia) en dr. J.A. van Wilsem (Universitair Hoofddocent Criminologie, Universiteit Leiden).

Voor dit onderzoek zijn veel publieke en private organisaties evenals onderwijsinstellingen geraadpleegd. In interviews met werkgevers, werknemers, onderwijsaanbieders en experts op het terrein van cybersecurity kwam grote interesse in het door ons onderzochte arbeidsmarktvraagstuk naar voren. De geïnterviewden toonden grote bereidheid om een bijdrage te leveren aan ons onderzoek. Hun inzet en openheid heeft het onderzoeksteam zeer op prijs gesteld.

In dit rapport wordt onder andere beschreven welke discrepanties tussen vraag en aanbod van CSP's op de korte en (middel)lange termijn kunnen worden verwacht. Ook worden verschillende oplossingsrichtingen voor deze discrepanties aangegeven. Samen kunnen deze bijdragen aan een meer duurzame goede balans van vraag en aanbod op de arbeidsmarkt voor CSP's.

Namens het onderzoeksteam,

Dr. J.A. van Lakerveld

PLATO BV (Universiteit Leiden)

Inhoudsopgave

Afkortingen 6
Samenvatting 7
1 Inleiding en achtergrond van het onderzoek 15
1.1 Inleiding op het onderzoek en leeswijzer 15
1.2 Achtergrond Cyberdreigingen en kwetsbaarheden 15
1.3 Initiatieven aanpakken cyberdreigingen 18
1.4 Probleemstelling en onderzoeksvragen 20
1.5 Onderzoeksopzet en -aanpak 22
2 Het werkveld van de Cyber Security Professionals en conceptueel kader 27
2.1 Definitie cybersecurity 27
2.2 Wie zijn de Cyber Security Professionals? 29
2.3 Karakteristieken onderwijs en opleiding 32
2.4 Discrepanties op de arbeidsmarkt 33
3 De vraag op de arbeidsmarkt naar Cyber Security Professionals 35
3.1 Arbeidsmarkt: overzicht totaal en vergelijking met ICT 35
3.2 Arbeidsmarkt voor technisch dominante specialistische cybersecurityfuncties (functiegroep 1) 41
3.3 Arbeidsmarkt voor niet technisch dominante specialistische cybersecurityfuncties (functiegroep 2) 46
3.4 Arbeidsmarkt technisch dominante functies waarbij cybersecurity een onderdeel is (functiegroep 3) 52
3.5 Arbeidsmarkt niet technisch dominante functies waarbij cybersecurity een onderdeel is (functiegroep 4) 56
3.6 Afsluitende opmerkingen 60
4 Aanbod van Cyber Security Professionals: onderwijs en opleiding 63
4.1 Beschikbaarheid van informatie over onderwijs en deelname 63
4.2 Overzicht van cybersecurity-gerelateerde onderwijs- en opleidingstrajecten 64
4.3 Duiding van het aanbod en overstijgende kwesties 72
5 Discrepanties op de arbeidsmarkt en oplossingsrichtingen 75
5.1 Inleiding model discrepantieanalyse: relateren vraag en aanbod 75
5.2 Discrepantieanalyse per functiegroep 78
6 Conclusies 91
6.1 Conclusies 91
6.2 Slotconclusie 97
Bijlage 1: Literatuuroverzicht 99
Bijlage 2: Overzicht geraadpleegde organisaties 105
Bijlage 3: Bijeenkomst Experts 109
Bijlage 4: Summary 111

Afkortingen

BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
CAP	Certified Authorization Professional
CBS	Centraal Bureau voor de Statistiek
CSP	Cyber Security Professional
CS	Cyber Security
CISSP	Certified Information Systems Security Professional
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CSSLP	Certified Secure Software Lifecycle Professional
CSR	Cyber Security Raad
DNS SEC	Domain Name System Security Extensions
EC3	European Cybercrime Centre
ECABO	Economisch en Administratief Beroeps Onderwijs
NCSC	Nationaal Cyber Security Centrum
IP	Internet Protocol
IT	Informatie Technologie
ICT	Informatie en Communicatie Technologie
ISACA	Information Systems Audit and Control Association
GDPR	General Data Protection Regulation
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Centrum voor Terrorismebestrijding en Veiligheid
NCSS	Nationale Cyber Security Strategy
NICE	National Initiative for Cybersecurity Education
RAND	Research and Development (denktank VS)
ROA	Researchcentrum Onderwijs en Arbeidsmarkt
SASBA	Sherwood Applied Business Security Architecture
SBB	Samenwerking Beroepsonderwijs Bedrijfsleven
SCADA	Supervisory Control And Data Acquisition)
SOC	Security Operation Centres
UWV	Uitvoeringsinstituut Werknemersverzekeringen
WODC	Wetenschappelijk Onderzoeks- en Documentatie Centrum
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Samenvatting

Aanleiding en doel van het onderzoek

Een tekort aan Cyber Security Professionals (CSP's) is een grote kwetsbaarheid voor de weerbaarheid van de vitale sectoren. In de "Nationale Cybersecurity Strategie 2 (NCSS2): Van bewust naar bekwaam" (2013) wordt benadrukt dat het Kabinet over voldoende cybersecuritykennis en –kunde wil beschikken. In dit kader is het van belang dat er op de korte en op de (middel)lange termijn evenwicht is tussen vraag en aanbod op de arbeidsmarkt voor CSP's binnen de publieke en private organisaties. Daarom wil de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) inzicht krijgen in de aard en omvang van een (eventueel) tekort aan deze professionals (zowel technisch als niet technisch) en oplossingsrichtingen identificeren om deze eventuele tekorten op korte en (middel)lange termijn te reduceren. In dit kader heeft PLATO BV van de Universiteit Leiden in samenwerking met Ockham IPS een arbeidsmarktonderzoek uitgevoerd naar vraag en aanbod van Cyber Security Professionals. Dit onderzoek is uitgevoerd in opdracht van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (WODC).

Onderzoeksvragen

In dit onderzoek staan de volgende onderzoeksvragen centraal:

- In hoeverre is er, nu en in de toekomst, een mogelijk kwalitatief en kwantitatief tekort aan Cyber Security Professionals op hoger en middelbaar niveau te verwachten?
- Hoe kunnen deze tekorten op de huidige en toekomstige arbeidsmarkt voor Cyber Security Professionals worden opgelost?

Onderzoeksopzet en –aanpak

De arbeidsmarkt voor CSP's wordt in dit onderzoek benaderd als een domein waar de vraag naar en het aanbod van professionals op het terrein van cybersecurity samenkomen en elkaar (proberen te) vinden. Bij het verkrijgen van inzicht over de vraagkant ligt in dit onderzoek het accent op vacature-analyse. Wat betreft de aanbodkant spitst het onderzoek zich toe op het onderwijs- en opleidingsaanbod.

Om vanuit verschillende relevante invalshoeken en bronnen antwoord te krijgen op de onderzoeksvragen, zijn ook andere methoden gebruikt. Het onderzoek bestond uit de volgende (deels overlappende) componenten:

- Literatuuronderzoek naar cybersecurity, het werkveld, kenmerken en functieprofielen van CSP's. Dit betrof beleidsliteratuur en wetenschappelijke literatuur zowel Nederlandse als internationale literatuur.
- Analyse van de maatschappelijke context en ontwikkelingen (politiek, economisch, sociaal, technologisch en juridisch) die van invloed zijn op de vraag naar en het aanbod van CSP's.
- Vacature-onderzoek (met behulp van vacaturespider Jobfeed[1] van Textkernel).
- Inventarisatie en analyse van het onderwijs- en opleidingsaanbod en inventarisatie van aantallen studenten. In dit kader is internetresearch uitgevoerd en zijn 18 onderwijsaanbieders geraadpleegd (door middel van 18 interviews, deels face-to-face en deels telefonisch).
- Verkennende en verdiepende interviews (deels face-to-face en deels telefonisch) met werkgevers, werknemers in het private en publieke domein. Hierbij ging het in totaal om 34 interviews verspreid over 25 organisaties.
- Expertmeeting. Deze bijeenkomst werd gehouden in de afrondende fase van het onderzoek, met als doel de gevonden discrepanties tussen vraag en aanbod en oplossingsrichtingen te bespreken. Bij de expertmeeting waren 7 deelnemers uit deze verschillende organisaties betrokken.

[1] http://www.jobfeed.nl/

Cybersecurity

Cybersecurity is geen eenduidig begrip. Bij in de literatuur gevonden definities van cybersecurity ligt vaak een accent op informatiebeveiliging en ICT. Cybersecurity moet niet te beperkt worden opgevat. Het begrip cybersecurity refereert aan de kwetsbaarheid van bedrijven, burgers, overheid en de maatschappij als geheel. Aan deze kwetsbaarheden en het oplossen daarvan, zitten zowel technische ICT-aspecten als interactie-aspecten (mens-ICT). Dit maakt cybersecurity niet alleen een technisch ICT-vraagstuk, maar vooral ook een organisatievraagstuk.

Conclusies 1: Cybersecurity is zowel een ICT- als een organisatievraagstuk. Cybersecurity moet vooral ook bekeken worden vanuit een breder organisatieperspectief waarin verschillende rollen en taken te vervullen zijn.

Het werkveld van Cyber Security Professionals

Het werkveld van de Cyber Security Professionals is sterk onderhevig aan veranderingen. De snel veranderende digitale wereld met daarbij komende dreigingen en noodzakelijke veiligheidscriteria stelt hoge eisen aan publieke en private organisaties om cybersecure te zijn of te worden. Zowel de frequentie van incidenten, als de impact daarvan, in termen van directe schade en indirecte schade (bijvoorbeeld imagoschade), neemt toe. Bedrijven en publieke organisaties worden zich meer en meer bewust van het feit dat cybersecurity niet alleen een ICT-issue is, maar een integraal thema. Cybersecurity is van een ICT-vraagstuk een 'boardroom issue' geworden, want het voortbestaan van het bedrijf kan in het geding komen. Toenemende beleidsaandacht voor cybersecurity, de noodzaak zich bewust te zijn van de risico's (aangezien internet zich op alle terreinen van het dagelijkse leven manifesteert) en veranderingen in wetgeving (op het gebied van privacy en dataprotectie) hebben een extra stuwend effect op de vraagontwikkeling.

Conclusie 2: Twee factoren houden het werkveld van de Cyber Security Professional sterk in beweging. Enerzijds gaat het hierbij om maatschappelijke ontwikkelingen (op politiek, economisch, sociaal, technisch en juridisch terrein). Anderzijds vragen incidenten (afhankelijk van frequentie en impact) om aanpassingen in het werkveld.

Functiegroepen

In de literatuur komen drie dimensies naar voren waarmee functies van Cyber Security Professionals kunnen worden beschreven:

- Werkzaamheden kunnen als *technisch dominant* of als *niet technisch dominant* worden getypeerd. Technisch dominant wil zeggen dat de nadruk ligt op het ICT-perspectief. Bij niet technisch dominante functies staat het organisatieperspectief meer centraal.
- De functie kan *specifiek op cybersecurity gericht* zijn of *cybersecurity als onderdeel* hebben.
- De functie kan *operationeel-tactisch* of *tactisch-strategisch* georiënteerd zijn.

Op basis van deze dimensies en bestudering van vacatureteksten kunnen vier groepen van functies worden onderscheiden:

1) *Technisch dominante specialistische cybersecurityfuncties*. Deze functies zijn zeer specifiek op IT/informatiebeveiliging gericht en hebben een grote technische component. Voorbeelden van functies zijn: ethical hackers, penetratietesters, software testers en technical security-engineers.
2) *Niet technisch dominante specialistische cybersecurity functies.* Hierbij gaat het om cyberspecialisten die meer vanuit een organisatieperspectief naar se-

curity kijken. Voorbeelden van functies zijn: IT security officers, IT security specialists, security officers, Information security officers, informatiebeveiligers.

3) *Technisch dominante functies waarbij cybersecurity een onderdeel is*. Deze beroepen zijn technisch van aard, maar niet gespecialiseerd in cybersecurity. Het betreft een brede groep beroepen waarvoor veelal een cybersecurity-gerelateerd certificaat vereist is of als pré wordt aangemerkt. Voorbeelden van functies zijn: systeembeheerders, softwareontwikkelaars en architects.

4) Niet technisch dominante functies waarbij cybersecurity een onderdeel is. Dit is de minst afgebakende functiegroep. Hierin bevinden zich tal van functies zoals beleidsmedewerkers, juristen, directeuren, auditors. Bij deze functies kan cybersecurity onderwerp van de kernactiviteit zijn (bijvoorbeeld jurist in privacy-issues, beleidsmedewerker op het gebied van cybersecurity). Daarnaast gaat het om functies waarin cyber eerder als object van een ander domein wordt gezien (bijvoorbeeld object van beleid, rechtspraak) dan als kern van de werkzaamheden.

Het onderscheid operationeel-tactisch en tactisch-strategisch komt in alle vier de functiegroepen terug

Conclusie 3: Op basis van de literatuur en bestudering van vacatureteksten, worden voor de Cyber Security Professional vier functieprofielen onderscheiden die in het kader van arbeidsmarktonderzoek gebruikt kunnen worden:

- *technisch dominante specialistische cybersecurityfuncties*;
- *niet technisch dominante specialistische cybersecurityfuncties;*
- *technisch dominante functies waarbij cybersecurity een onderdeel is;*
- *niet technisch dominante functies waarbij cybersecurity een onderdeel is.*

De vraag naar en totale werkgelegenheid voor Cyber Security Professionals

In de eerste drie kwartalen van 2014 zijn in totaal 916 vacatures gepubliceerd met betrekking tot het cybersecuritydomein. Op jaarbasis (gerekend over het laatste kwartaal van 2013 en de eerste drie kwartalen van 2014) gaat het om 1.158 gepubliceerde vacatures op het gebied van cybersecurity. De totale vraag zal groter zijn, omdat informele wervingskanalen en challenges[2] gericht op werving niet als vacatures tellen in de vacature-analyse.

Om een indruk te krijgen van de totale werkgelegenheid (het totaal aantal arbeidsplaatsen) op het gebied van cybersecurity maken we een vergelijking met de aantallen gepubliceerde vacatures en de werkgelegenheid in de brede ICT-sector. In de brede ICT-sector staat één vacature tot zes arbeidsplaatsen.[3] Passen we deze zelfde verhouding tussen vacatures en arbeidsplaatsen toe op het cybersecuritydomein, dan wordt op basis hiervan de totale werkgelegenheid binnen het cybersecuritydomein geschat op 7.000 arbeidsplaatsen.

Op basis van de omgevingsanalyse (het maatschappelijk belang en de rol van incidenten nemen toe, zie conclusie 2) wordt verwacht dat de vraag naar Cyber Security Professionals zal stijgen. Enerzijds neemt de urgentie van het inzetten van kennis en kunde op dit terrein toe. Anderzijds wordt het cybersecuritydomein steeds meer ook als een organisatievraagstuk gezien en breder opgevat (multidisciplinair).

De verwachte stijging van de vraag geldt voor alle vier de functiegroepen en ook voor aanpalende functies: Het cybersecuritydomein is een belangrijk deel van de leefwereld en

[2] Een 'challenge' wordt in dit onderzoek omschreven als een uitdagende wervingsactiviteit met een *gaming* karakter, waarbij vraagstukken op het terrein van cybersecurity moeten worden opgelost.

[3] In 2013 was de totale werkgelegenheid in de ICT/automatisering ongeveer 300.000 (Panteia op basis van P-Direkt en Enquête beroepsbevolking, CBS). Het totaal aantal vacatures op jaarbasis is ongeveer 50.000 (Panteia/PLATO op basis van vacatureanalyse Jobfeed). De verhouding tussen het aantal vacatures en de totale werkgelegenheid is daarom 1 : 6.

daarom zijn verschillende aanpalende functies nodig waarin kennis van cybersecurity onontbeerlijk is.
Er moet onderscheid worden gemaakt in de vraag naar functies op MBO-, HBO- en WO-niveau. Door digitalisering en automatisering neemt de vraag naar MBO-opgeleiden binnen de ICT af, de vraag naar hoger opgeleiden neemt juist toe.

Conclusie 4: Weliswaar is het aantal zichtbare vacatures momenteel nog bescheiden, echter er zijn indicaties (toename van de urgentie en bredere opvatting van het cybersecuritydomein) dat de vraag naar CSP's (in zijn totaliteit) in de toekomst zal toenemen. Deze stijging *geldt vooral voor hoger opgeleiden en in mindere mate voor op MBO-niveau opgeleide professionals.*

De aard van de vraag naar de vier in dit onderzoek onderscheiden functiegroepen laat zich als volgt typeren:

1) *Technisch dominante specialistische cybersecurityfuncties.* De arbeidsmarkt voor dit profiel wordt, naast grote werkgevers (zowel banken, politie en defensie) gedomineerd door consultancybedrijven. Deze specialisten (hackers, pentesters) delen met cybercriminelen de rol van 'front-runner' in de ontwikkeling van cybersecurity. Om de verdere technologische ontwikkeling van cybercrime bij te benen, zal de vraag naar deze specialisten aanhoudend stijgen.
2) *Niet technisch dominante specialistische cybersecurityfuncties.* De arbeidsmarkt voor dit functieprofiel kent een gedifferentieerder palet aan vragende organisaties. Het aanstellen van dit type CSP is voor veel organisaties de eerste stap in het op orde brengen van de cybersecurity. In veel gevallen is één CSP voldoende om de security te organiseren. Specialistische taken worden via inhuur van derden uitgevoerd. Na een sterke groei in de eerste vijf jaar zal de vraag naar niet technische dominante cybersecurityfuncties licht dalen, doordat organisaties hun beveiliging in de organisaties hebben ingebed. Tegen die tijd zal echter de vervangingsvraag ook een rol gaan spelen omdat mensen met pensien gaan. In vacatures met betrekking tot deze groep functies wordt om professionals met ervaring gevraagd.
3) *Technisch dominante functies waarbij cybersecurity een onderdeel is.* In de arbeidsmarkt voor dit functieprofiel wordt de grootste groei verwacht. Deze markt wordt bepaald door software-ontwikkelaars. Deze bedrijven zijn zich de laatste jaren gaan toeleggen op verbeterde beveiliging van hun software (secure by design) en vragen ICT'ers met ervaring op het terrein van security, securitycertificaten en/of -affiniteit. Aangezien meer en meer organisaties als softwarebedrijven gezien kunnen worden (ICT is de kern van veel bedrijven), neemt de vraag naar deze technici in de toekomst toe. De vraag naar veiligere systemen weerklinkt in de systeemontwikkeling en systeembeheersing.
4) *Niet technisch dominante functies waarbij cybersecurity een onderdeel is.* De arbeidsmarkt voor dit functieprofiel kent een veelheid aan verschillende functies, waarbij sommige professionals niet eens beseffen dat zij zich bezighouden met cybersecurity. In de toekomst zullen vaker en nadrukkelijker competenties ten aanzien van cybersecurity-gerelateerde taken worden gevraagd.

Conclusie 5: Een stijging van de vraag geldt voor alle functiegroepen, maar de grootste groei wordt verwacht bij de technisch dominante functies waarbij cybersecurity een onderdeel is.

Aanbod van Cyber Security Professionals vanuit onderwijs en opleiding

Er zijn in dit onderzoek ruim tachtig soorten aanbod geïnventariseerd. Als het aantal aanbiedingslocaties daarin wordt verwerkt, gaat het om vele honderden opleidingen en andere vormen van aanbod. Het opleidingsaanbod gerelateerd aan cybersecurity is zeer

divers en omvangrijk. Er bestaan veel aanbiedingsvormen naast elkaar, zoals initiële opleidingen, post-initieel onderwijs, korte cursussen, masterclasses, workshops, seminars, on the job leren, afstandsonderwijs, en in-company training.
De opleidingen worden op talrijke locaties aangeboden. Er zijn initiële en post-initiële opleidingen van MBO- tot WO-niveau. Ook in de private sector is het aanbod groot. Hierbij ligt een accent op het up-to-date houden van kennis en vaardigheden van werkenden.

Ook voor wat betreft inhoud en diepgang is de range van het aanbod breed. Deze bestrijkt opleidingen met duidelijke technische en informatica-inhouden én opleidingen met duidelijke veiligheids-, juridische, of forensische inhouden. Ook zijn er opleidingen die deelnemers indirect, maar diepgaand scholen in voor cybersecurity relevante vakken en competenties. In die categorie vallen opleidingen die een sterke ICT-component hebben maar gericht zijn op andere dan technische- of veiligheidsgebieden, zoals kunstmatige intelligentie, studies methoden en technieken, medische informatiekunde, logistiek, meet- en regeltechniek, etc. Al met al is er een veel breder aantal opleidingen dat aan de kennis en kunde van studenten/deelnemers bijdraagt, dan alleen de direct op ICT-, of internet- en cybersecurity gerichte opleidingen.

De veelheid aan opleidingen, cursussen en aanbiedingsvormen leidt ook tot intransparantie van het aanbod. Informatie over onderwijs- en opleidingstrajecten is op zich wel te achterhalen, maar wat ontbreekt is één helder overzicht van de opleidingsmogelijkheden en -routes in relatie tot de competenties waarvoor deelnemers willen en/of moeten worden opgeleid.

Conclusie 6: Het opleidingsaanbod gerelateerd aan cybersecurity is divers en omvangrijk. Opleidingen worden vaak op verschillende locaties aangeboden en er is veel variatie in aanbiedingsvormen. Tegelijkertijd is het aanbod weinig transparant.

Wat betreft het aanbod van professionals vanuit onderwijs en opleiding, lijken er in 2014 ruim voldoende deelnemers in een relevante vooropleiding te zitten:

- een instroom van 6.880 deelnemers op MBO 4 niveau;
- een instroom van 73 deelnemers op HBO associate degree niveau;
- een instroom van 4.053 deelnemers op HBO niveau;
- een instroom van 292 deelnemers op Master niveau;
- een instroom van deelnemers aan post-academische- en post-executive masters van (zoals blijkt uit de interviews) zeker 200 personen.

Er is dus een groot potentieel aan mensen die in principe inzetbaar lijken. Zelfs als we rekening houden met een uitval van 50%, blijven de aantallen nog hoog in vergelijking met de beschikbare vacatures. Tegelijkertijd leiden deze aantallen maar zeer beperkt tot instroom in cybersecurity-gerelateerde functies. MBO'ers vervolgen hun opleiding vaak op HBO-niveau. Veel bredere HBO- en WO-opleidingen hebben cybersecurity maar beperkt in het programma ingebouwd en er zijn (nog) weinig specialistische cybersecurity-opleidingen. Dit leidt ertoe dat studenten niet of pas relatief laat cybersecurity als optie meenemen in hun overwegingen ten aanzien van hun verdere studie of loopbaan.

Conclusie 7: Het opleidingspotentieel is in principe toereikend om te voorzien in de vraag naar CSP's. Het is echter de vraag of deelnemers aan cybersecurity-gerelateerde opleidingen cybersecurity als loopbaanoptie zien.

Gevonden discrepanties tussen vraag en aanbod

Gevonden discrepanties bij onderzoeksvraag 1: In hoeverre is er, nu en in de toekomst, een mogelijk kwalitatief en kwantitatief tekort aan Cyber Security Professionals op hoger en middelbaar niveau te verwachten?

In de relatie van de vraag naar en het aanbod van CSP's zijn eerder intransparanties en kwalitatieve discrepanties te constateren dan kwantitatieve discrepanties. De opgave lijkt niet zozeer te zijn om meer mensen op te leiden, maar veeleer om hen tijdens hun opleiding te interesseren voor cybersecurity en voor banen in die sector. De aansluitingsproblemen (discrepanties tussen vraag en aanbod) die organisaties ervaren, zijn eerder van kwalitatieve dan van kwantitatieve aard of te wijten aan intransparantie van de arbeidsmarkt. Samengevat komen de volgende discrepanties naar voren:

- Studenten worden weliswaar opgeleid in voor cybersecurity relevante studierichtingen, maar zij missen een specifieke gerichtheid op cybersecurity.
- Veel organisaties hebben onvoldoende kennis over wat zij eigenlijk nodig hebben, wie ze precies zoeken en waar ze die kunnen vinden.
- Er is voldoende aanbod, maar de professionals hebben nog niet het gewenste niveau: zij missen (afhankelijk van de functie en de taken) òf technische kennis òf kennis van de organisatie.
- Professionals hebben cybersecurity als deeltaak erbij gekregen, maar zijn niet specifiek opgeleid op dat terrein. Omdat zij veel andere taken hebben ligt snelle competentie-ontwikkeling op het terrein van cybersecurity ook niet altijd voor de hand.

Conclusie 8: In kwantitatieve zin hoeft er geen sprake te zijn van tekorten. De aansluiting van de vraag naar CSP's en het aanbod van deze professionals wordt gehinderd door intransparanties en kwalitatieve discrepanties.

Oplossingsrichtingen bij de gevonden discrepanties

Hierbij gaat het om de beantwoording van onderzoeksvraag 2: Hoe kunnen (eventueel) geconstateerde tekorten op de huidige en toekomstige arbeidsmarkt voor Cyber Security Professionals worden opgelost? Met andere woorden: Hoe kan de match tussen vraag en aanbod worden verbeterd? In het onderzoek komen de volgende (mede door experts op het terrein van cybersecurity benadrukte) oplossingsrichtingen naar voren:

1. De mogelijkheden van het onderwijs benutten bij het oplossen van discrepanties.
Het onderwijs kan een grote rol spelen bij het oplossen van discrepanties. Het gaat daarbij om het bevorderen van bewustzijn onder leerlingen en studenten in het algemeen, het motiveren tot voor cybersecurity relevante studiekeuzes bij een deel van de leerlingen en studenten en het gericht, zelfs specialistisch, opleiden van een nog specifiekere groep. Leren en professionaliseren in een zich snel ontwikkelend veld als de cybersecurity vereist bij uitstek een vorm van een leven lang leren. In het kader van een leven lang leren is het van belang, ook te zoeken naar efficiënte en effectieve manieren om in werksituaties de kennis verder te ontwikkelen, te delen en te vertalen in verbeteringen en innovaties. De werkomgeving strekt verder dan alleen de eigen organisatie.

Behalve professionalisering in de zin van persoonlijke ontwikkeling in het beroep, is er ook de noodzaak van ontwikkeling van het vak. Cybersecurity is een terrein waar op verschillende niveaus, veel werk wordt verricht in allerlei publieke en private organisaties (van klein tot groot) en industrieën. Ook de opleidingswereld draagt bij aan de ontwikkelingen in het cybersecuritydomein. Samenwerking van alle betrokken partijen is van vitaal belang voor het 'up to date' blijven van de cybersecuritysector en allen die daarin werkzaam zijn. We zien dit vertaald in actieve betrokkenheid van ICT-bedrijven in opleidingen, in deelname van practici als docenten in hogere opleidingen, en in participatie van wetenschappers in het oplossen van praktische problemen.

2. *Veranderen van werkprocessen in organisaties en samenwerking tussen organisaties, om zodoende het niveau van cybersecurity op peil te brengen en te houden.*

In het onderzoek in zijn totaliteit komen op dit vlak de volgende mogelijkheden naar voren:

- gelegenheid creëren binnen en tussen organisaties om kennis te delen en van elkaar te leren;
- verbeteren van secundaire arbeidsvoorwaarden, wat het werk voor meer groepen zoals vrouwen, extra aantrekkelijk kan maken;
- efficiënter en gerichter werven (ook binnen de eigen organisatie, door functionarissen opmerkzaam te maken op de mogelijkheden om door te groeien in een cyber cybersecurity-gerelateerde functie);
- inzet van een pool van professionals vanuit verschillende organisaties, outsourcing en inhuren van externe specialisten;
- zichtbaar maken van het werk van de CSP binnen de organisatie en het nut daarvan;
- hanteren van een minder hiërarchische organisatiestructuur (geldt voor grotere organisaties).

3. *Verhelderen van onderwijs- en opleidingsroutes.*

De relatie tussen opleidingstrajecten en –routes, te verwerven competenties, uit te oefenen functies en te bereiken posities op de arbeidsmarkt is diffuus. De trajecten die loopbaanontwikkeling in de cybersecurity ondersteunen zijn dat ook. Keuzes maken in het woud van mogelijkheden is niet altijd eenvoudig. Daar ondervinden zowel de mensen die het aangaat als de organisaties de nadelen van. Het betekent dat te vaak de juiste man of vrouw op de verkeerde plek belandt. Het leidt tot inefficiënte en ineffectieve leer- en loopbaanroutes. Het verhelderen van de onderwijs- en opleidingstrajecten en –routes, zal een positieve uitwerking hebben op de kwaliteit van het aanbod en de toeleiding van uitstromende deelnemers en studenten naar functies op het terrein van cybersecurity.
Deze oplossingsrichting verwijst ook naar een leven lang leren. Het werkveld van cybersecurity vraagt om permanente actualisering van kennis en het 'up to date' houden van vaardigheden. In dat kader groeit de noodzaak om gestalte te geven aan een systeem van onderhoud van kennis, actualisering van kennis en kennisontwikkeling.

4. *Monitoren van ontwikkelingen in de samenleving, het onderwijs en opleidingen en arbeidsmarkt. De hierdoor verkregen gegevens kunnen de aansluiting van de vraag naar en het aanbod van CSP's op de korte en (middel)lange termijn ten goede komen.*

In het verlengde van oplossingsrichting 3 kan dataverzameling en registratie over opleidingen en de vraag op de arbeidsmarkt een bruikbaar middel voor kwaliteitsverbetering zijn. Het onderzoek naar de arbeidsmarkt voor Cyber Security Professionals, zoals beschreven in dit rapport, biedt een stand van zaken. De samenleving in zijn totaliteit en het werkgebied van de CSP's zijn sterk in beweging. Een vorm van monitoring van ontwikkelingen in de samenleving, de arbeidsmarkt en de opleidingsmarkt kan de aansluiting van de vraag naar en het aanbod van CSP's op de kortere en langere termijn ten goede komen.

5. *Het imago van het cybersecuritywerkveld en de -functies sterker en uitdagender neerzetten.*

Cybersecurityfuncties worden nog al eens geassocieerd met een bepaald soort ethical hackers die volledig opgaan in hun vak (zwart T-shirt, paardenstaart etc.). Aan de andere kant worden cybersecurityfuncties in verband gebracht met 'moeilijkdoeners binnen de organisatie': immers door hun oriëntatie op alles wat er mis kan gaan, zijn zij in de ogen van anderen wel een beetje moeilijk. De uitdagende, vooruitstrevende, en complexe aspecten van het werk mogen meer op de voorgrond worden gebracht. Een andere kwestie is dat de sector vooral uit mannen bestaat. Op het terrein van cybersecurity zijn verschillende functies te vervullen waarbij verschillende soorten competenties vereist zijn. Dat maakt het werkveld interessant voor mannen en vrouwen. Een positieve uitstraling van

de mogelijkheden en uitdagingen maakt de vijver waaruit kan worden gevist groter. Voorlichting, scholing en eventueel publieksacties (bijvoorbeeld in de vorm van challenges) kunnen ook bijdragen aan verandering.

6. *Cybersecurity oppakken als een gezamenlijke verantwoordelijkheid van burgers, overheid, organisaties en onderwijs: gericht op bewustwording.*

Alle geraadpleegde organisaties en deskundigen zijn het erover eens: cybersecurity is een kwestie die het leven van vrijwel iedere burger beïnvloedt. Daarom is het belangrijk om gericht op de hele samenleving, te werken aan bewustwording. Het doel hiervan is dat iedereen zich bewust wordt van de risico's en de mogelijkheden zich daartegen te weer te stellen. Er ontstaat aldus een behoefte om deskundigen op te leiden en in te zetten, die die bredere groep van burgers weten te bereiken met de boodschap dat cybersecurity vraagt om alertheid, maatregelen en controles op het gebied van informatieveiligheid.

Dit houdt ook in dat cybersecurity meer gezien moet worden als iets wat altijd en overal een rol speelt waar mensen met ICT-systemen werken en interacteren. Hierin ligt ook een taak voor het funderend onderwijs (primair en secundair onderwijs). Hoe daaraan vorm te geven, zal in toekomstig onderzoek verder moeten worden uitgezocht.

Conclusie 9: Oplossingsrichtingen voor discrepanties op de arbeidsmarkt voor CSP's hebben betrekking op:

1. *Benutten van de mogelijkheden van onderwijs en opleidingen op het vlak van (o.a.) bewustwording, studiekeuze, verduidelijken van opleidingsroutes en mogelijkheden voor een leven lang leren op het terrein van cybersecurity.*
2. *Versterken en verbeteren van werkprocessen in organisaties en bevorderen van samenwerking tussen organisaties.*
3. *Verhelderen van onderwijs- en opleidingsroutes.*
4. *Monitoren van ontwikkelingen in relatie tot de arbeidsmarkt van CSP's.*
5. *Verbeteren en versterken van het imago van het cybersecuritywerkveld en de CSP.*
6. *Doorgaan op de ingeslagen weg om cybersecurity te benaderen als een gezamenlijke verantwoordelijkheid van burgers, overheid, organisaties, onderwijs en opleidingen: gericht op bewustwording.*

1 Inleiding en achtergrond van het onderzoek

1.1 Inleiding op het onderzoek en leeswijzer

Een tekort aan Cyber Security Professionals (CSP's) is een grote kwetsbaarheid voor de weerbaarheid van de vitale sectoren. In de "Nationale Cybersecurity Strategie 2 (NCSS2): Van bewust naar bekwaam" (2013) wordt benadrukt dat het Kabinet over voldoende cybersecuritykennis en –kunde wil beschikken. In dit kader is het van belang dat er op de korte en op de langere termijn evenwicht is tussen vraag en aanbod op de arbeidsmarkt voor CSP's binnen de publieke en private organisaties. Daarom wil de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) inzicht krijgen in de aard en omvang van een (eventueel) tekort aan deze professionals (zowel technisch als niet technisch) en oplossingsrichtingen identificeren om deze eventuele tekorten op korte en middellange termijn te reduceren. In dit kader heeft PLATO BV van de Universiteit Leiden in samenwerking met Ockham IPS een arbeidsmarktonderzoek verricht naar vraag en aanbod van Cyber Security Professionals. Dit onderzoek is uitgevoerd in opdracht van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (WODC).

In dit hoofdstuk wordt allereerst nader ingegaan op de achtergrond van het onderzoek. Aan de orde komen cyberdreigingen en kwetsbaarheden in de samenleving, bij bedrijven en burgers. Ook wordt beschreven welke initiatieven en aanpakken er zijn ontwikkeld om kwetsbaarheden en dreigingen het hoofd te bieden. Daarna volgen de probleemstelling en de onderzoeksvragen die in dit onderzoek centraal staan en tot slot wordt de onderzoeksopzet en –aanpak toegelicht.

In aansluiting op dit eerste hoofdstuk bevat deze rapportage de volgende hoofdstukken:

- Het werkveld van de CSP's en conceptueel kader (hoofdstuk 2).
- De vraag naar CSP's op de arbeidsmarkt (hoofdstuk 3).
- Het aanbod van CSP's: onderwijs en opleiding (hoofdstuk 4).
- Discrepanties en oplossingsrichtingen (hoofdstuk 5).
- Conclusies (hoofdstuk 6).

In de bijlagen zijn opgenomen: een literatuuroverzicht, een overzicht van geraadpleegde organisaties en opleidingsaanbieders, informatie over de expertmeeting die in de afrondende fase van het onderzoek is gehouden en een Engelstalige samenvatting.

1.2 Achtergrond Cyberdreigingen en kwetsbaarheden

De technologische ontwikkelingen gaan razend snel. De bedrijvigheid op internet stijgt explosief, burgers leven meer en meer online en ook de overheid manifesteert zich in toenemende mate op het internet. Dit brengt nieuwe verschijningsvormen van bestaande ongemakken met zich mee, zoals cyberpesten, cyberfraude, cybercrime en cyberwar. Niet alleen bedrijven, burgers en overheden bevinden zich in het cyberdomein, maar ook criminelen. Meer en meer criminaliteit speelt zich af in het cyberdomein. Het is dan ook van belang dat bedrijven, burgers en overheden voldoende beschermd zijn. Hierdoor neemt het belang én de noodzaak van cybersecurity nu en in de toekomst alleen maar toe.

- Ten eerste breidt het cyberdomein zich meer en meer uit. We zien softwaretoepassingen op zo mogelijk alle domeinen van menselijk handelen terugkomen (internet of things).[4] Waar enkele jaren geleden internet grote, logge PC's in grijze kasten verbond, zijn inmiddels miljarden apparaten (telefoons, tablets, PC's, in-

[4] http://www.ictmarktmonitor.nl/ict-marktmonitor-2014/nieuwe-technologieen/#5

ternetradio's, IP-camera's, sensoren, wasmachines, koelkasten, lantaarnpalen, stoplichten) met het internet verbonden. In totaal waren er in 2012 ongeveer 9 miljard objecten die op de één of andere manier verbonden waren met het internet.[5] Dit brengt meer veiligheidsrisico's met zich mee.

- Ten tweede zijn nieuwe technologieën geïntroduceerd zonder voldoende de veiligheidsrisico's in de toekomst in ogenschouw te nemen (Committee on Professionalizing the Nation's Cybersecurity Workforce, 2014). Vooral software-gerelateerde technologieën zijn kwetsbaar door de onvermijdelijke programmeerfouten (Bos; 2013).[6] Dit gegeven kan enerzijds aanleiding zijn voor een toename aan cybergerelateerde criminaliteit: oude systemen blijven immers jaren in de lucht en zijn moeilijk aan te passen[7]. Anderzijds kan het ook een aanleiding zijn voor een afname van criminaliteit, doordat huidige ICT-technologieën meer rekenschap afleggen aan huidige én zo mogelijk toekomstige veiligheidsrisico's (Committee on Professionalizing the Nation's Cyber Security Workforce, 2014).

Deze ontwikkelingen hebben hun weerslag op de kwetsbaarheid van organisaties en bedrijven, burgers en de samenleving als geheel (zie hieronder).

1.2.1 Kwetsbaarheid bedrijven

Ondanks dat de kosten van cybercrime lastig in kaart zijn te brengen (Anderson et al. 2012)[8], zijn er verschillende inschattingen gemaakt. Symantec schatte de economische schade (op basis van een onderzoek in 24 landen verspreid over Australië en Nieuw Zeeland, Europa, Noord- en Zuid Amerika, het Midden Oosten en Azie) op 110 miljard US dollars per jaar (Symantec 2012[9]). Het Britse Detica schat de kosten van cybercrime in het VK op 27 miljard pond.[10] TNO heeft, mede op basis van andere schattingen, ook een inschatting voor Nederland gemaakt. Deze komt uit op 10 miljard per jaar.[11] RAND becijferde de kosten van cyberaanvallen voor het Europese bedrijfsleven op 4 miljard Euro[12]. Zeer recentelijk (2014) becijferde de virusscanner McAfee de totale kosten in Nederland op 8.8 miljard per jaar.[13] Probleem met al deze inschattingen is, dat het lastig is om een onderscheid te maken tussen directe en indirecte (beveiligings)kosten (Anderson et al. 2012)[14]. De kosten komen voornamelijk terecht bij het bedrijfsleven (Detica, 2011) en bedrijven zullen zich meer en meer moeten organiseren om risico's ter verminderen.

Echter, met de toenemende dreiging en kosten neemt ook de weerbaarheid en het herstelvermogen van bedrijven en organisaties toe (FD, 24 augustus, interview Dick Schoof). Er is een toenemende nadruk op 'Security by design', maar ook op verbeterde veiligheidsprotocollen (bijvoorbeeld IPv6, het Secure Border Gateway Protocol en DNS-

[5] http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342
[6] Bos, H, "We hebben hackers nodig" in: Magazine Nationale veiligheid en crisisbeheersing, jaargang 11, nummer 6 december Den Haag 2013.
[7] Denk bijvoorbeeld aan de informatiesystemen van levensverzekeraars. Zij moeten de informatie decennia beschikbaar hebben.
[8] Anderson, R., et al., 2012. Measuring the cost of cybercrime. Workshop on the Economics of Information Security (WEIS) [online]. Available from: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf [Accessed 10 December 2014].
[9] Symantec, 2012. Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually [online]. Available from: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 [Accessed 10 December 2012].
[10] Detica (2011). The Cost of Cyber Crime.
[11] NRC Next beoordeelt deze inschatting echter als ongefundeerd: http://www.nrcnext.nl/blog/2012/05/01/next-checkt-%E2%80%98cybercrime-kost-nederland-jaarlijks-zeker-10-miljard%E2%80%99/
[12] http://digizine.fd.nl/outlook-special-april2014/
[13] Zie persbericht: http://www.persberichten.com/persbericht/78450/Onderzoek-McAfee-cybercriminaliteit-kost-de-Nederlandse-economie-jaarlijks-ruim-8-8-miljard-euro; Center for Strategic and International Studies (2014), Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II.
[14] Anderson, R., et al. (2012). Measuring the cost of cybercrime. Workshop on the Economics of Information Security (WEIS) [online]. Available from: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf [Accessed 10December 2014].

SEC[15]).[16] Desondanks, lijken vele voorbeelden toch het tegendeel te bewijzen: ook huidige systemen zijn kwetsbaar voor hackers.[17] Daarnaast is door standaardisering in programmatuur misschien de kans op een lek verkleind, maar de impact van een lek is hierdoor juist vergroot (zie bijvoorbeeld de Open SSL Heartbleed bug).[18] Ook is het technisch gemakkelijker geworden om te hacken, een cybercrime te plegen. Daar staat tegenover dat het óók technisch makkelijker is met incidenten om te gaan. Tenslotte vertoont security irrationaliteiten (Hoogenboom, 2012).[19] Betere beveiliging leidt tot verwaarlozing in de vorm van achterstallig onderhoud van systemen; oude patches die doordraaien en niet of te laat worden vervangen; scans die niet optimaal functioneren; de monitoring van systemen en processen die zwak is ontwikkeld.[20]

Gegeven de directe en indirecte kosten (bijvoorbeeld ook reputatieschade), zijn bedrijven zich meer en meer bewust geworden van het feit dat cybersecurity niet alleen een ICT-issue is, maar een integraal thema. Cybersecurity is van een ICT-vraagstuk een boardroom issue geworden, want het voortbestaan van het bedrijf kan in het geding komen.[21] Dit zorgt ervoor dat cybersecurity een organisatievraagstuk is geworden. Echter deze beweging is meer in het grootbedrijf terug te zien dan in het Midden en Klein Bedrijf (MKB). Deze laatste groep bedrijven is zich nog onvoldoende bewust van cyber risico's.[22]

Daarnaast zouden bedrijven security meer in termen van een competitief voordeel moeten zien dat hun beveiliging op orde is in plaats van een kostenpost (FD, 24 augustus, interview Dick Schoof). Dit moet ook bezien worden in het licht van veranderende wetgeving. De Europese Unie werkt aan de nieuwe EU General Data Protection Regulation (GDPR), een nieuwe wet die organisaties verplicht hun data beter te beschermen. Drie op de vijf bedrijven voldoet op dit moment nog niet aan de eisen die deze nieuwe regelgeving gaat stellen. Dit blijkt uit onderzoek van Kroll Ontrack en Blancco onder 660 IT-managers in Europa. De nieuwe Europese wet treedt naar verwachting pas in 2016 in werking. Bedrijven zullen zich echter nu alvast moeten gaan voorbereiden om op tijd te voldoen aan de wetgeving. Slechts twee op de vijf bedrijven heeft op dit moment al maatregelen genomen met het oog op de nieuwe regelgeving. Dit is niet verwonderlijk, aangezien vier op de vijf IT-managers niet bekend blijkt te zijn met de nieuwe wetgeving. IT-beslissers zullen nog flink wat kennis moeten opdoen om zich goed te kunnen voorbereiden op de regels.[23] Deze cijfers betreffen Europa, in hoeverre de Nederlandse situatie hiermee overeenkomt, of van afwijkt, is onduidelijk.

1.2.2 Kwetsbaarheid burgers

Gegeven de technologische mogelijkheden van ICT en het gebruik ervan door burgers, zijn burgers in toenemende mate kwetsbaar voor cybercrime[24]. Het rapport 'Cyber Security Perspectives 2013' beschrijft dit als een opkomende trend voor 2014 (NCSC, 2013).[25] De reden hiervoor is de toename van 'connected pieces of equipment', waarbij het niet alleen gaat om computers, camera's en telefoons, maar ook om koelkasten, wasmachines en andere huishoudelijke apparaten. Een gemiddeld huishouden heeft 10 tot 30 ap-

[15] Deze (en soortgelijke) protocollen zorgen voor een inherent veiliger inrichting van het internet als geheel. Wel zal een zorgvuldige en wereldwijde implementatie nodig zijn om de optimale effecten hiervan te bereiken.
[16] Advies CSR dd 31-07-2013: https://www.ncsc.nl/organisatie/samenwerkingspartners/publiek-privaat/csr.html.
[17] Zie: Meulen, N.S. van der, Lodder, A.R., (2014). Cybersecurity (hoofdstuk 13), in: S. van der Hof, A.R. Lodder, G.J. Zwenne (Ed.), Recht en Computer (6e druk) (pp. 301-318). Deventer: Kluwer: voorbeelden Patiëntendossier, aanvallen op banken. Andere voorbeelden: OV-chipkaart.
[18] http://nl.wikipedia.org/wiki/Heartbleed
[19] Hoogenboom, B. (2012). Cyber Security Dialogen.
[20] Hoogenboom, B. (2012). Cyber Security Dialogen.
[21] http://digizine.fd.nl/outlook-special-april2014/
[22] Zie bijvoorbeeld: http://www.mkbservicedesk.nl/8818/wat-zijn-cyber-security-trends-voor-2014.htm
[23] http://dutchitchannel.nl/517839/europese-bedrijfsleven-is-niet-klaar-voor-nieuwe-europese-datawetgeving.html
[24] Naast cybercrime spelen ook andere cyberfenomenen een rol in de kwestbaarheid van burgers, zoals cyberpesten.
[25] NCSC, (2013), Cyber Security Perspectives 2013.

paraten met een IP-adres (NCSC, 2013)[26]. Ook maken meer en meer mensen gebruik van internetbankieren en gebruiken zij apps op hun mobiele telefoon. Internet dringt diep door in ons alledaagse en persoonlijke en publieke leven, met als consequentie dat individuen op deze gebieden kwetsbaar zijn: we kunnen via internet worden bedreigd, bespioneerd, afgeperst, bestolen en beschadigd.[27]

Deze afhankelijkheid vertaalt zich niet vanzelfsprekend in kennis en bewustzijn van de risico's.[28] Beleidsinitiatieven worden genomen om dit bewustzijn en digitale geletterdheid te vergroten. In het advies van de Cyber Security Raad (CSR) wordt benadrukt dat "[…] de burger als individuele gebruiker van het digitale domein meer bewust moet omgaan met veiligheid en privacy en daartoe ook veel meer dan momenteel het geval is in de gelegenheid moet worden gesteld. Daarbij hoort, naast een bewustwordingscampagne en meer transparantie over het gebruik van persoonsgegevens, ook het investeren in onderwijs rondom veilig en effectief gebruik van ICT".[29]

1.2.3 Kwetsbaarheid samenleving

Volgens de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) hebben we als samenleving als geheel nog niet goed in de gaten wat de gevolgen zijn van een toenemende digitalisering (WRR, 2011).[30] De grenzen tussen overheidsinstanties, beleidsvelden en tussen de overheid en de markt worden in rap tempo beslecht waardoor ook de verantwoordelijkheid voor het aanpakken van overstijgende problemen onduidelijker wordt. En, de toename van cyberincidenten duidt daarnaast op de kwetsbaarheid van deze digitale stromen. Volgens de WRR staan we nog maar aan het begin van het doordenken van de gevolgen van de toenemende grensvervagingen en toenemende kwetsbaarheden van dit proces.[31]

Tenslotte is een veilige ICT-omgeving belangrijk voor het vestigingsklimaat.[32] Investeren in een veilige infrastructuur is een economische noodzaak.

1.3 Initiatieven aanpakken cyberdreigingen

De kwetsbaarheid van overheidsstructuren en vitale systemen staat in de aandacht. Daarnaast zijn bedrijven, publieke organisaties en individuen vaker slachtoffer van cybercrime. Hierdoor staat cybersecurity in veel landen hoog op de politieke agenda. Naast Europese initiatieven (zoals het EC3) ontwikkelen de Europese lidstaten en andere landen nationale cybersecuritystrategieën (RAND, 2013)[33]. Er kan zelfs gesproken worden van een overbevolkte beleidsruimte.

---

[26] NCSC, (2013), Cyber Security Perspectives 2013.
[27] http://www.sociosite.org/cyberoorlog.php
[28] Zie burgers bewustzijn: http://www.trendsinveiligheid.nl/
[29] Advies CSR dd 31-07-2013: https://www.ncsc.nl/organisatie/samenwerkingspartners/publiek-privaat/csr.html. Zie hiervoor ook het KNAW-rapport "Digitale geletterdheid in het voortgezet onderwijs", via www.knaw.nl. In zekere zin ligt deze gevoeligheid voor cybersecurity al vervat in het Europese Raamwerk van sleutelcompetenties voor een leven lang leren: "digital competence involves the confident and critical use of information society technology (IST) and thus basic skills in information and communication technology (ICT)" (Recommendation 2006/962/EC of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning [Official Journal L 394 of 30.12.2006]. "Digitale competentie omvat de vertrouwdheid met en het kritische gebruik van technologieën van de informatiemaatschappij voor het werk, in de vrije tijd en voor communicatie. Zij wordt onderbouwd door basisvaardigheden in ICT: het gebruik van computers om informatie op te vragen, te beoordelen, op te slaan, te produceren, te presenteren en uit te wisselen, en om via internet te communiceren en deel te nemen aan samenwerkingsnetwerken."). Echter in de beschrijving van deze sleutelcompetentie ontbreekt een referentie naar veilig gebruik.
[30] WRR, (2011), iOverheid.
[31] Zie: Hoogenboom, B. (2012). Cyber Security Dialogen.
[32] Groeien door veiligheid: een onderzoek naar de waarde van een veilige en betrouwbare ICT-infrastructuur voor de Nederlandse economie- Ernst & Young, 2011.
[33] RAND (2013). Cyber-security threat characterisation: A rapid comparative analysis

Ook in Nederland zijn de laatste jaren door diverse instanties verschillende beleidsdocumenten en -strategieën geproduceerd die het gevaar benoemen van cybercrime en het belang van actief beleid om deze vorm van criminaliteit te beteugelen.

In Nederland is de Nationale Cyber Security Raad per 1 januari 2012 actief en in 2014 is de Nationale Cyber Security Strategie (NCSS) 2 gepubliceerd. Aanpassen van kwetsbare systemen is een gezamenlijke verantwoordelijkheid van overheid, bedrijfsleven en individuen. Daarom wordt in het aanpakken van cybercrime vanuit een publiek-privaat partnerschap gewerkt.[34] Deze nadruk op samenwerking toont een al langer gaande verschuiving van de verantwoordelijkheid voor veiligheid van de overheid naar burgers en bedrijven.[35] Dit betreft niet alleen de verantwoordelijkheid voor de eigen systemen (van burgers en bedrijven), maar ook een oplettendheid ten opzichte van de systemen van de overheid. Iedereen die zwakke plekken in de ICT-systemen van de overheid tegenkomt wordt gevraagd deze te melden (Responsible Disclosure[36]).

Volgens de 'Nationale Cybersecurity Strategie 2: van bewust naar bekwaam' (NCSS 2) wordt cybersecurity gedefinieerd als 'het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan'. Deze schade aan ICT kan bestaan uit de aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid (Ministerie van Veiligheid en Justitie 2013).

Het aanpakken van cybercrime speelt zich af op het snijvlak van overheid, bedrijfsleven en burger. De cybersecurityaanpak (NSCC2) heeft daarbij een drieledig doel dat overheid, bedrijfsleven én burger direct raakt, namelijk:[37]

1) *Het garanderen van veiligheid*: Cybersecurity gaat zowel om de veiligheid van ICT als om de veiligheid van daarin opgeslagen informatie.
2) *Vrijheid*: Fundamentele rechten en waarden moeten worden beschermd.
3) *Maatschappelijke groei*: De innoverende kracht die uitgaat van verdergaande digitalisering is een belangrijke stimulans voor maatschappelijke groei. Het gaat daarbij zowel om economische groei als om de mogelijkheden die digitalisering biedt aan de samenleving, bijvoorbeeld in de vorm van onderwijstoepassingen, mogelijkheden tot het onderhouden van sociale contacten en verbeterde overheidsvoorzieningen.

Eén van de cybersecuritydoelstellingen van het Kabinet is dan ook dat Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie (zoals verwoord in doelstelling 5, Nationale Cybersecurity Strategie 2, Ministerie van Veiligheid en Justitie 2013). Voldoende Cyber Security Professionals (CSP's) zijn nodig om enerzijds optimaal gebruik te kunnen maken van de kansen die digitalisering ons biedt en anderzijds ons weerbaar te maken tegen de steeds geavanceerdere dreigingen. CSP's zijn daarnaast hard nodig om cybersecurityoplossingen voor de toekomst te ontwerpen en te bouwen. Het gaat hierbij om de beschikbaarheid van voldoende en kwalitatief goede CSP's binnen publieke en private organisaties. Een tekort aan CSP's gaat gepaard met de nodige risico's voor vitale (digitale) systemen die van belang zijn voor de Nederlandse economie, veiligheid en vrijheid van burgers.

Ondanks het belang van deze technische CSP's, geven studies (bv. CapGemini 2013) weinig cijfermatig inzicht in aspecten van CSP's, zoals: het aantal werkzame CSP's in

[34] Zie verslag van de informele bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 18-19 juli 2013 te Vilnius.
[35] Zie Bob Hoogenboom, Cyber Security Dialogen, verwijzing naar het rapport 'Samenleving en criminaliteit' (1985).
[36] http://www.rijksoverheid.nl/onderwerpen/cybercrime/cybercriminaliteit-bestrijden/responsible-disclosure
[37] Zie: Ministerie van Veiligheid en Justitie (2013). De Nationale Cybersecurity Strategie (NCSS) 2 Van bewust naar bekwaam: http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2.html

Nederland; de karakteristieken van deze CSP's (bijvoorbeeld hun onderwijsachtergrond en leeftijd); de competenties waarover zij beschikken; het dienstverband waarin zij werken (loondienst, zzp'er); hun loopbaanperspectieven. Ook is er weinig cijfermatig inzicht over de aansluiting van het aanbod van CSP's op de vraagzijde van de arbeidsmarkt en hoe deze vraagzijde zich door de jaren heen ontwikkelt.

1.4 Probleemstelling en onderzoeksvragen

Op basis van het voorgaande kan de probleemstelling voor het onderzoek op de volgende wijze beknopt worden samengevat: Om zowel op de korte als (middel)lange termijn optimaal gebruik te kunnen maken van de kansen die digitalisering ons biedt en weerbaar te zijn tegen de steeds geavanceerdere dreigingen, zijn voldoende kwalitatief goede CSP's nodig. Een tekort aan CSP's gaat gepaard met de nodige risico's voor vitale (digitale) systemen die van belang zijn voor de Nederlandse economie, veiligheid en vrijheid van burgers. Tegelijkertijd is er weinig bekend over de huidige stand van zaken en prognoses ten aanzien van de arbeidsmarkt voor CSP's. Met dit onderzoek wil de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) inzicht krijgen in de aard en omvang van het tekort aan Cyber Security Professionals (zowel technisch als niet technisch) en oplossingsrichtingen identificeren om deze tekorten op korte en middellange termijn te reduceren.

In dit onderzoek staan de volgende onderzoeksvragen centraal:

1) In hoeverre is er, nu en in de toekomst, een mogelijk kwalitatief en kwantitatief tekort aan Cyber Security Professionals op hoger en middelbaar niveau te verwachten?
2) Hoe kunnen deze tekorten op de huidige en toekomstige arbeidsmarkt voor Cyber Security Professionals worden opgelost?

Daarbij zijn de volgende deelonderzoeksvragen geformuleerd:

A: Kenmerken cybersecurity en Cyber Security Professionals

1. *Wat wordt er verstaan (definities) onder cybersecurity en CSP's?*
2. *Welke soorten cybersecurityspecialisten kunnen worden onderscheiden?*
3. *Welke functie- en competentie-eisen worden er aan CSP's gesteld (en welke kwalificatie- en certificatie-eisen)?*
4. *Wat zijn achtergrondkenmerken van CSP's in termen van: opleidingsniveau, type opleiding, werkervaring, arbeidsmarktstatus (loondienst of zzp'er; inkomensniveau; imago professie) en demografische kenmerken (leeftijdsopbouw; geslacht)?*

B: Invloed van omgevingsfactoren op arbeidsmarkt CSP's

5. *Wat is de huidige en toekomstige situatie ten aanzien van politieke, economische, sociaal-maatschappelijke, technologische en wettelijke ontwikkelingen die van invloed zijn op de arbeidsmarkt van CSP's?*
6. *Wat is er in grote lijnen bekend over de actuele en toekomstige ontwikkelingen op het terrein van de digitale veiligheid (in het publieke en private domein)?*
7. *Welke mogelijke implicaties hebben deze ontwikkelingen voor de huidige respectievelijk toekomstige CSP's (in het publieke en private domein) gerelateerd aan vraagstukken met betrekking tot digitale veiligheid?*

C: Vraag naar CSP's

8. *Wat is de aard en omvang van de vraag (vacatures) naar CSP's op de korte, middellange en lange termijn (hoeveel en welke kennis, kunde, competenties en/of sociale vaardigheden)?*
9. *Wat is de verwachte vervangingsvraag en uitbreidingsvraag in de toekomst?*

10. *Hoe vertaalt deze vraag zich naar de verschillende soorten cybersecurityspecialisten?*
11. *Hoe ziet de aard en omvang van de vraagzijde van de arbeidsmarkt van CSP's eruit, gespecificeerd naar typen werkgevers in het publieke domein (bijvoorbeeld centrale en decentrale overheid, politie, defensie) en het private domein (bijvoorbeeld bedrijfsleven waaronder ICT-sector, banken, telecom, vitale infrastructuur)? In welke sectoren is de vraag het grootst?*

D: Aanbod aan CSP

12. *Hoeveel CSP's zijn op dit moment werkzaam in de sector (gespecificeerd naar functiecategorie)?*
13. *Wat is het totale aanbod aan CSP's voor de korte, middellange en lange termijn (aantal huidige studenten met relevante opleiding, afgestudeerde werkzoekenden, onbenut potentieel overige beroepsbevolking)?*
14. *Welke onderwijsrichtingen en opleidingen zijn er op het terrein van cybersecurity (initieel en post-initieel)?*
15. *Hoeveel studenten staan ingeschreven voor deze opleidingen en wanneer en met hoeveel komen deze studenten op de arbeidsmarkt?*
16. *Hoe ziet het aanbod van deze onderwijsrichtingen en opleidingen eruit in relatie tot de functie- en competentie-eisen van werkgevers?*
17. *Hoe kan de internationale arbeidsmarkt voor CSP's een bijdrage leveren aan het mogelijke tekort aan CSP's in Nederland?*

E: Discrepanties op de arbeidsmarkt (vraag en aanbod)

18. *Wat zijn de kwantitatieve discrepanties?*
    - *Hoe verhouden de kwantitatieve vraag- en aanbodzijde van de arbeidsmarkt zich ten aanzien van CSP's op korte, middellange en lange termijn? In hoeverre kunnen de huidige studenten voorzien in de totale behoefte aan CSP's op de arbeidsmarkt voor de korte, middellange en lange termijn?*
    - *Met betrekking tot welke professionals treden tekorten/overschotten op, op korte, middellange en lange termijn?*
    - *Waar zijn knelpunten aan te wijzen ten aanzien van de kwantitatieve instroom in de sector?*
19. *Wat zijn de kwalitatieve discrepanties?*
    - *Hoe verhouden zich het aanbod van en de vraag naar competenties ten aanzien van CSP's op korte, middellange en lange termijn?*
    - *Met betrekking tot welke competenties treden tekorten/overschotten op, op korte, middellange en lange termijn?*
    - *Waar zijn knelpunten aan te wijzen ten aanzien van de kwalitatieve instroom in de sector?*
20. *In hoeverre is de arbeidsmarkt ondoorzichtig? In hoeverre is het onderwijs (aanbod) afgestemd op de arbeidsmarkt (vraag)? In hoeverre bestaat er bijvoorbeeld een uitwisseling van enerzijds kennis en mensen uit de wetenschap (ICT) zoals AIO's en post-doc's en anderzijds van kennis en mensen uit het bedrijfsleven en de overheid?*

F: Oplossingsrichtingen

21. *In hoeverre kunnen (initieel) onderwijs-gerelateerde activiteiten knelpunten wegnemen? Is er in de toekomst een tekort aan opleidingsplaatsen? Zo ja, hoe groot is dit tekort?*
22. *In hoeverre kan post-initieel onderwijs/ scholing van werkenden knelpunten wegnemen?*
23. *In hoeverre kunnen aanpassingen van de bedrijfsactiviteiten een oplossing bieden? In hoeverre kunnen verbetering van primaire en secundaire arbeidsvoorwaarden discrepanties wegnemen? Dient het imago van de sector verbeterd te worden? Kan het verplaatsen van bedrijfsactiviteiten een oplossing bieden (internationaal)? Wat zijn specifieke knelpunten hierin?*

24. *In hoeverre kan internationaal werven een bijdrage leveren aan het oplossen van knelpunten? Wat zijn de specifieke knelpunten bij internationaal werven (bv. arbeidsvergunningen)?*
25. *Welke rol spelen verschillende betrokken actoren, zoals publieke en private partijen (Nederlandse bedrijfsleven, waaronder de ICT-sector; ministeries van OCW, SoZaWe en VenJ) bij het implementeren van mogelijke oplossingsrichtingen (organiserend vermogen / rol stakeholders)?*
26. *Zijn er goede praktijken uit andere sectoren/landen die als inspiratie kunnen dienen voor het oplossen van knelpunten?*

1.5 Onderzoeksopzet en -aanpak

In dit onderzoek zijn verschillende bronnen en onderzoeksmethodieken gebruikt om de onderzoeksuitkomsten gedegen te onderbouwen en vanuit alle relevante invalshoeken uitspraken te kunnen doen over het functioneren van de arbeidsmarkt van CSP's.
Deze methoden zijn:

- literatuuronderzoek;
- vacature-analyse;
- inventarisatie en analyse van het onderwijsaanbod;
- interviews: verkennende interviews en verdiepende interviews met werkgevers, werknemers en onderwijsaanbieders;
- expertmeeting.

1.5.1 Literatuuronderzoek

De literatuurstudie was gericht op het verkrijgen van inzicht in:

- definities en omschrijvingen van 'cybersecurity' en 'Cyber Security Professionals';
- verkenning van verschillende soorten cyber security professionals, uitgesplitst naar aard van werkzaamheden (technisch, juridisch, beleidsmatig) en/of sector waarin zij werkzaam zijn (publieke domein – private domein);
- functie- en competentie-eisen aan (soorten) CSP's;
- omgevingsfactoren die de arbeidsmarkt voor CSP's beïnvloeden. Deze betreffen ondermeer:
  - huidige politieke, economische, sociaal-maatschappelijke/demografische, technologische, juridische ontwikkelingen die inspelen op de sector (publieke en private sector);
  - toekomstige ontwikkelingen op deze terreinen (publieke en private sector);
  - actuele en toekomstige ontwikkelingen op het terrein van digitale veiligheid, (publieke en private sector).

Ook is in de literatuur gezocht naar implicaties van omgevingsfactoren en ontwikkelingen in het cybersecuritydomein voor de huidige of toekomstige eisen aan (soorten) cybersecurity professionals.

In het onderzoek is zowel beleidsliteratuur als wetenschappelijke literatuur en zowel nationale- als internationale literatuur geraadpleegd. In bijlage 1 is een literatuuroverzicht opgenomen.

De literatuurstudie vond deels gelijktijdig plaats met de *verkennende interviews*. Voorafgaand en tijdens deze interviews vroegen we respondenten om bronnen te noemen die we in de literatuurstudie zouden moeten worden meegenomen.

1.5.2 Vacatureanalyse

Op de arbeidsmarkt voor Cybersecurity Professionals is sprake van interactie tussen de vraag naar en het aanbod van deze professionals. Het is een abstract domein waar vraag

en aanbod samen (kunnen) komen. De analyse van de arbeidsmarkt in dit onderzoek is gericht op het identificeren van discrepanties die zich hierbij voordoen. De onderzoekers hebben in dit kader een vacature-analyse uitgevoerd waarbij de kwalitatieve en kwantitatieve vraag naar CSP's in kaart is gebracht. Hiervoor zijn vacaturegegevens uit de database van vacaturespider Jobfeed[38] van Textkernel gebruikt. Jobfeed doorzoekt dagelijks het internet naar nieuwe vacatures, ontdubbeld deze (vacatures worden vaak op meerdere plaatsen geplaatst), extraheert informatie als beroep, opleiding, locatie en bedrijfsnaam uit de vacatures en structureert deze in een database. Op deze database kunnen complexe zoekopdrachten worden uitgevoerd.

Representativiteit van jobfeed
Met de vacaturespider Jobfeed registreert Textkernel meer dan 99% van alle vacatures op het Nederlandse internet. Wat betreft het ICT-segment is Jobfeed hiermee representatief voor alle vacature-uitingen in Nederland en vervolgens voor alle ingevulde vrijgekomen ICT arbeidsplaatsen in Nederland[39], óók gegeven het feit dat personen instromen zonder dat er een vacature extern is opengesteld. Het aantal personen dat jaarlijks instroomt op de arbeidsmarkt of een andere baan vindt volgens het CBS ligt ongeveer anderhalf keer zo hoog als het aantal extern geworven vacatures. De instroom vindt in dat geval plaats via relaties, via bestanden met open sollicitaties, via een stage of leerbaan. Onderzoek van Panteia in 2012 heeft opgeleverd dat dit percentage in de sector zorg en welzijn nog hoger ligt dan elders. Organisaties die op die manier een medewerker aannemen, hebben vaak ook via internet geworven. Gemiddeld zet men meer dan twee wervingskanalen per vacature in[40]. In onderzoek van het UWV[41] naar de bemiddeling van vacatures, is ook vastgesteld dat bedrijven eerder kiezen voor de via-via route, of voor een via een open sollicitatie binnengekomen sollicitant dan voor het aannemen van personeel via een ander kanaal. Over het ICT-segment bestaan geen cijfers. Het vermoeden bestaat echter, bijvoorbeeld bij ECABO,[42] dat werkgevers in dat segment eerder vacatures op het internet plaatsen dan werkgevers in andere segmenten van de arbeidsmarkt.

Het identificeren van CSP-gerelateerde vacatures
Hierbij zijn onderstaande stappen doorlopen:

1) De Jobfeed database is op drie manieren doorzocht op cybersecurity-relevante vacatures:
   - Naar functienaam: geselecteerde brede beroepen zijn: security officer en IT security specialist.
   - Naar cybersecurity-gerelateerde certificaten: de volgende certificaten zijn gebruikt om de database te doorzoeken: CISSP, CISM, CISA, CRSC, CEH
   - Naar cybersecurity-gerelateerde kernwoorden: de volgende kernwoorden zijn gebruikt: ethical hacker, cyber, informatiebeveilig…, IT security.
2) Op basis van deze zoekopdrachten zijn in totaal bijna 4.300 relevante vacatures geïdentificeerd over de laatste twee jaar (van 23-09-2012 tot 01-10-2014).
3) In Jobfeed bevinden zich vacatures die direct door bedrijven zijn gepubliceerd, maar ook vacatures die door intermediaire partijen worden aangeboden. Vacatures die via intermediairs als uitzendbureaus (Randstad, Tempo Team, USG, etc.), wervings- en selectiebureaus (Brunel, Hunt IT, IT-Staffing), headhunters, etc.

[38] http://www.jobfeed.nl/
[39] Bij de eerste pilot naar de inzet van Jobfeed als meetinstrument om het aantal vacatures te bepalen waarvoor extern wordt geworven (2010-2011) is vastgesteld dat Jobfeed gemiddeld ongeveer 70% van de extern geworven vacatures die het CBS door middel van haar vacature-enquête meet, vaststelt. Bij levering van de aantallen vacatures aan het UWV en de stichting SBB wordt hiervoor door Panteia gecorrigeerd door middel van weging. In het ICT-segment is weging echter niet nodig, omdat Jobfeed ongeveer evenveel vacatures registreert als het CBS. Het CBS heeft in 2012 vastgesteld dat vrijwel alle bedrijven en instellingen die extern voor vacatures werven dat in ieder geval ook via internet doen. In een onderzoek voor de stichting SBB in 2013 heeft Panteia vervolgens vastgesteld dat de bedrijven die via internet werven ongeveer 85-90 procent van hun externe vacatures ook daadwerkelijk op internet zetten.
[40] UWV (2014), Vacatures in Nederland 2013 de vacaturemarkt en personeelswerving in beeld.
[41] UWV (2014), Vacatures in Nederland 2013 de vacaturemarkt en personeelswerving in beeld.
[42] Kenniscentrum beroepsonderwijs bedrijfsleven voor de economisch/administratieve, ICT- en veiligheidsberoepen.

worden aangeboden zijn uit de selectie gehaald. Dit omdat vaak niet te achterhalen is of het bij de verschillende intermediairs om dezelfde vacature gaat (en omdat we ze ook niet kunnen vergelijken met de originele vacatures van de bedrijven en instellingen), zijn deze vacatures niet goed te tellen. Na het weglaten van deze intermediair aangeboden vacatures blijven ongeveer 2.200 vacatures over.

4) Namen van beroepen en functies zijn niet (altijd) gestandaardiseerd. Om deze reden is een aantal beroepen gehercodeerd op basis van het inzien van de vacatureteksten.
5) Functies en beroepen die minder dan drie keer gevraagd zijn in de afgelopen twee jaar zijn buiten beschouwing gelaten in de verdiepende analyses (functie-eisen, organisaties, arbeidsvoorwaarden. Het gaat hierbij in totaal om ongeveer 180 vacatures.

De analyse van de vacaturegegevens van Jobfeed is deels kwantitatief en deels kwalitatief van aard. Voor de afgelopen twee jaar is het aantal vacatures voor CSP's, voor verschillende cybersecurity-geralateerde functiegroepen, in kaart gebracht. In aanvulling op deze kwantitatieve analyses zijn ook meer kwalitatief getinte analyses uitgevoerd op de vacaturegegevens van Jobfeed. Het gaat daarbij om een inhoudelijke analyse van de vacatureteksten. De uitkomst van de vacature-analyse is zowel een kwantitatief overzicht van de vraag (opleiding, opleidingsniveau, type werkgevers, locatie werkgevers etc.), als een kwalitatief overzicht van de vraag (type werkzaamheden, ervaring en specifieke gevraagde competenties).

De kwantitatieve analyse van aantallen vacatures en de kwalitatieve analyse van vacatureteksten zijn verdiept aan de hand van interviews met werkgevers en werknemers. Dit wordt nader toegelicht in paragraaf 1.5.5.

Ten aanzien van de vacature-analyse moet tot slot het volgende worden opgemerkt:

- Er zijn geen gestandaardiseerde functieprofielen die eenduidig een bepaald beroep of functie aanduiden.
- Functies die in een meer aansturende rol zitten, of functies die in de periferie van cybersecurity zitten, zijn lastig af te bakenen.
- Aangezien het overgrote deel van vacatures online wordt aangeboden, is geen wegingsfactor toegepast om te compenseren voor anders aangeboden vacatures (zoals kranten en geschreven media). Dit neemt niet weg dat voor het werven van CCP's ook wel eens gebruik wordt gemaakt van andere wervingskanalen (zoals hacketons, cybersecurity challenges en het direct benaderen op de universiteit). Echter in veel gevallen is de vacature ook op internet te vinden.

1.5.3 Inventarisatie en analyse van het onderwijsaanbod

Om beter zicht te krijgen op de aanbodzijde van de arbeidsmarkt, zijn de bestaande onderwijs- en opleidingstrajecten[43] van waaruit mensen doorstromen naar de functie van CSP bestudeerd. Er zijn zowel reguliere opleidingen (zoals MBO-, HBO- en WO-opleidingen) meegenomen, als aanbieders van 'losse' cursussen en trainingen. De focus was gericht op technische trajecten en bredere opleidingen waarbinnen voor een deel aandacht wordt besteed aan cybersecurity.

De inventarisatie van het aanbod startte met verkennende interviews die aan het begin van het onderzoek werden. Daarna volgde een uitgebreide internetsurvey. Voorbeelden van gebruikte zoektermen zijn: ICT-beveiliging, internetbeveiliging, informatiebeveiliging, internet security, cybersecurity, computerveiligheid/-beveiliging, cyber crime, cyber safety, information security officer, security engineer. Uit het overzicht van cybersecurity- gerelateerde opleidingen (meer dan tachtig) dat deze exercitie opleverde, is een se-

[43] We gebruiken de term 'trajecten' als overkoepelend begrip voor alle aanduidingen van onderwijs, zoals opleidingen, cursussen, modulen, trainingen en minors.

lectie van achttien aanbieders gemaakt.[44] Met de betreffende onderwijs- en opleidingsinstellingen zijn verdiepende telefonische interviews gehouden.

1.5.4 Interviews

In totaal zijn 25 (publieke en private) organisaties en 18 onderwijsaanbieders geraadpleegd. Er is in totaal met 52 respondenten (deels face-to-face en deels telefonisch) gesproken. In bijlage 2 is een overzicht opgenomen van alle geraadpleegde organisaties, onderwijsaanbieders en geïnterviewde.

Hieronder geven we een nadere toelichting op de verschillende soorten interviews.

1.5.4a verkennende interviews

Doel van deze interviews was oriënterend en gericht op het uitbreiden en aanscherpen van het beeld van de onderzoekers van de arbeidsmarkt voor CSP's, beroepsprofielen en het onderwijsaanbod op dit terrein. De interviews vonden plaats in de beginfase van het onderzoek, parallel aan de literatuurstudie. We vroegen respondenten om bronnen te noemen die in de literatuurstudie zouden moeten worden meegenomen. Aan de andere kant vormden bevindingen uit de literatuur input voor de gesprekken.
Gesprekken zijn gevoerd met beleidsadviseurs/-ontwikkelaars, wetenschappers, onderwijsexperts en experts op het terrein van cybersecurity die met een helicopterview het domein konden benaderen. Zowel het publieke als private domein was in de verkennende interviews vertegenwoordigd.

1.5.4b interviews met werkgevers en werknemers

De interviews met werkgevers en werknemers hadden tot doel: verdieping en duiding van verkregen resultaten en inzichten uit de kwantitatieve analyse van vacatures en de kwalitatieve analyse van vacatureteksten.
Bij de werkgevers spraken we met personeels- en/of HR-managers of lijnmanagers. Bij de werknemers ging het om gesprekken met verschillende CSP's die de verschillende beroepsprofielen van CSP vertegenwoordigen.
Onderwerpen die in de gesprakken met werkgevers aan de orde kwamen zijn:

- Kenmerken van de werkgevers, het werk en de werkzaamheden;
- Aantal CSP's;
- De vervangings- en uitbreidingsvraag van CSP's in de toekomst (1, 5 >5 jaar);
- Precisering vereiste competenties, kwalificaties en ervaring, ervaringen met sollicitanten van specifieke CSP opleidingen;
- Aantallen en kwaliteit van sollicitanten (achtergrond, opleidingen etc.);
- Vervullen vacatures (eventuele moeilijkheden);
- Wervingskanalen (online, headhunters, internationaal);
- Aanvullende on-the-job trainingstrajecten;
- Oplossingsmogelijkheden bij (dreigende) tekorten (zelf opleiden, internationaal werven, verplaatsen bedrijfsactiviteiten, outsourcen);
- Interessante praktijken in het buitenland/aanpalende sectoren m.b.t. omgang met de arbeidsmarkt voor CSP.[45]

In de interviews met werknemers (CSP's) stonden de volgende aspecten centraal:

- Opleiding(en);
- Werkervaring, loopbaanperspectief;
- Beeld van de sector, het beroep, de werkgever;
- Kanaal waarlangs huidige baan is gevonden (vacature, interne opleiding);
- Huidige werkzaamheden;
- Primaire en secundaire arbeidsvoorwaarden;

[44] Er zijn in dit onderzoek meer dan tachtig soorten aanbod geïnventariseerd, maar als het aantal aanbiedingslocaties daarin worden verwerkt, gaat het om vele honderden opleidingen en andere vormen van aanbod.
[45] NB: de laatste fase van het onderzoek gaan we interessante praktijken uit andere sectoren/landen nader bekijken (onderzoeksactiviteit 8).

- Carrière perspectieven.

1.5.4c interviews met onderwijsaanbieders

In totaal zijn 18 verdiepende interviews gehouden, verdeeld over reguliere MBO-, HBO- en WO instellingen en private onderwijsaanbieders. Vaak werden in een interview meerdere door de betreffende instelling geboden opleidingen, cursussen en/of trainingen op het terrein van of gerelateerd aan cybersecurity besproken.
Hoofdthema's in de interviews waren: type opleidingstraject en -niveau; aantal studenten en docenten; kenmerken van het programma (onder andere: onderdelen, vakken, eindtermen, competenties, studie duur en –last); in- en uitstroomgegevens; achtergrond docenten; ontwikkelingen en verwachtingen; relatie met arbeidsmarkt; kwaliteitsborging en externe validering van de opleiding.

1.5.6 Expertmeeting

Na de analyse van de vraag- en aanbodzijde, is een bijeenkomst met experts gehouden. Het doel van deze bijeenkomst was de bevindingen terug te koppelen aan een brede groep stakeholders en met hen oplossingsrichtingen bij de gevonden discrepanties tussen vraag en aanbod op de arbeidsmarkt van CSP's te bespreken. Het programma voor de bijeenkomst was opgezet volgens de *Delphi methode.* Een belangrijk kenmerk van deze methode is de herhaalde raadpleging van deskundigen waarbij de resultaten tussentijds worden gerapporteerd. Dit vormt dan weer de inzet voor een nieuwe ronde raadpleging enzovoorts. Opeenvolgende rondes van raadplegen van experts bouwen zo op elkaar voort.
Ruim vijfentwintig experts waren voor deze bijeenkomst uitgenodigd. Hoewel alle benaderde experts zich zeer geïnteresseerd toonden in het onderzoek, waren uiteindelijk slechts zeven van hen daadwerkelijk in de gelegenheid om deel te nemen. Veel van de genodigden die niet konden komen, vroegen of zij alsnog op andere wijze een bijdrage aan het onderzoek konden leveren.
In bijlage 3 is een beschrijving van de opzet, werkwijze en opbrengst van de expertmeeting opgenomen. De resultaten van de bijeenkomst zijn integraal verwerkt in hoofdstuk 5 van dit rapport.

2 Het werkveld van de Cyber Security Professionals en conceptueel kader

In dit hoofdstuk worden op basis van het literatuuronderzoek en interviews enkele centrale begrippen met betrekking tot cybersecurity verhelderd. Wat is cybersecurity? Wie zijn CSP's? Hoe ziet hun functie eruit en welke functiegroepen zijn te onderscheiden? Daarna wordt een kader geschetst voor hoe in dit onderzoek (in respectievelijk hoofdstuk 3 en 4) een beeld wordt verkregen van de vraag naar CSP's en het aanbod van CSP's.

2.1 Definitie cybersecurity

De term 'cybersecurity' deed zijn intrede kort na het begin van het nieuwe millennium. Inmiddels is het begrip breed geadopteerd en wordt er steeds vaker en meer over geschreven. Wat daarbij opvalt, is dat de term veelal gebruikt wordt zonder dat daarbij een duidelijke omschrijving wordt gegeven. Vaak worden in relatie tot cybersecurity verschillende begrippen en omschrijvingen gehanteerd. Daarbij wordt het begrip soms als synoniem gebruikt voor, of in verband gebracht met, termen als: cybercrime, cybersafety, informatieveiligheid, informatiebeveiliging, digitale veiligheid, cyberterrorisme. Deze begrippen op zich worden in verschillende studies ook weer verschillend gedefinieerd (o.a. Leukfeldt en Stol 2012; Van der Meulen 2014; Kessler en Ramsey 2013; Spruit en Van Noord 2014).[46]

Verschillen in definiëring worden mede veroorzaakt door de verschillende invalshoeken van waaruit het domein wordt beschreven zoals technische, beleidsmatige, criminologische, economische en juridische[47] invalshoeken. De afgelopen jaren is ook een steeds groter accent komen te liggen op cybersecurity als strategisch concept, met als doel de nationale veiligheid te waarborgen/verdedigen.[48] Daarbij wordt verwezen naar een divers palet aan dreigingen waarmee verschillende partijen, van individuele gebruikers tot aan overheidsinstanties en vitale bedrijven, worden geconfronteerd zoals:

1) *Informatiegerelateerde dreigingen*: informatie verkrijgen, misbruiken, publiceren en/of veranderen;
2) *Systeemgerelateerde dreigingen*: de dienstverlening of bedrijfsvoering van een organisatie verstoren;
3) *Indirecte dreigingen*: spill-over effect van eerder genoemde categorieën, waarbij ook andere gebruikers getroffen kunnen worden.

[46] Leukfeldt, E.R, Stol, W. (2012). Cybersafety: An introduction (pp. 23–30). Eleven International Publishing.
Meulen, N.S. van der, Lodder, A.R., (2014). Cybersecurity (hoofdstuk 13), in: S. van der Hof, A.R. Lodder, G.J. Zwenne (Ed.), Recht en Computer (6e druk) (pp. 301-318). Deventer: Kluwer.
Kessler, G.C., Ramsey, J. (2013). Paradigms for Cybersecurity Education, http://commons.erau.edu/cgi/viewcontent.cgi?article=1011&context=db-applied-aviation
Spruit, M., Van Noord, F. (2014). Beroepsprofielen Informatiebeveiliging, PvIB.

[47] Op juridisch vlak houdt de definitie van cybercrime verband met de instantie die bevoegd is dit tegen te gaan. Hierbij spelen discussies rond 'cyberwar' een grote rol. Cybercrime kan door individuen, organisaties, maar ook staten gepleegd worden. Cyber ar is hierbij het inzetten van internettoepassingen om oorlogshandelingen te verrichten, echter de term bevat ook de verdedigings- en interventiemechanismen om aanvallen tegen te gaan. Hiermee is cyber war een zeer complex en diffuus begrip (Boer, Lodder; 2012). Eenzelfde handeling door een verschillende entiteit (staat of individu) kan als oorlogshandeling of als criminele handeling worden geclassificeerd (zie ook Holt, 2012). Dit levert juridische problemen op, omdat afhankelijk van wie achter een daad zit een andere instantie (leger, openbaar ministerie, veiligheidsdienst, etc.) met andere bevoegdheden en vanuit andere beweegredenen bevoegd is (Van der Meulen, Lodder; 2014). Sinds 9/11 worden terroristische aanvallen ook als oorlogshandelingen behandeld.

[48] Geers, K. (2011), Strategic Cyber Security. NATO Cooperative Cyber Defense Centre for Excellence. Tallinn, Estonia.

Tot slot is er meer aandacht voor het belang van het stimuleren van het bewustzijn van de risico's en daarnaar handelen. Benadrukt wordt dat stakeholders, publieke en private organisaties en individuele gebruikers hier een verantwoordelijkheid hebben.[49]

Een eenduidige definitie van cybersecurity, waarbij ook wordt aangegeven hoe dit begrip zich verhoudt tot andere begrippen, is er niet. Van der Meulen en Lodder hebben in een bijdrage aan Recht en Computer (2014)[50] getracht het begrip cybersecurity nader af te bakenen t.a.v. het veelgebruikte begrip 'informatiebeveiliging'. Cybersecurity lijkt breder dan informatiebeveiliging. Immers, veiligheid op internet kan ook situaties omvatten die niet door beveiliging zijn op te lossen (denk bijvoorbeeld aan cyber bullying). Aan de andere kant lijkt informatiebeveiliging juist breder: informatiebeveiliging kan ook om beveiliging náást een netwerkomgeving gaan.

Voor dit arbeidsmarktonderzoek is een brede definitie het meest bruikbaar. De definitie van cybersecurity zoals gehanteerd in de Nationale Cyber Security Strategy 2 (NCSS 2) voldoet hieraan. Voor deze studie is deze definitie licht aangepast.[51]

Cybersecurity betreft het reduceren van gevaar of schade veroorzaakt door introductie van nieuwe technologie, storing of uitval van ICT of misbruik van ICT tot een aanvaardbaar risico.

Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.

In deze definitie wordt een verband gelegd met informatiebeveiliging en ICT. Hierdoor komen ook veel genoemde principes als *confidentiality* (vertrouwelijkheid), *integrity* (integriteit) en *availability* (beschikbaarheid) in beeld.

Vooruitlopend op de volgende paragraaf moet worden benadrukt dat de hierboven gegeven definitie cybersecurity nog iets te nadrukkelijk in de context van ICT plaatst. Cybersecurity moet vooral ook bekeken worden vanuit een breder organisatieperspectief waarin verschillende rollen en taken te vervullen zijn. Veilige ICT omgevingen zijn geen doel op zich, maar een middel om de kernprocessen van een organisatie veilig te laten verlopen. Hierbij is cybersecurity niet alleen afhankelijk van de ICT, maar juist van de mensen die er gebruik van maken en van de organisatorische inbedding van veiligheidsbewustzijn. Cybersecure zijn vraagt veel meer van organisaties dan enkel een veilige ICT omgeving neerzetten.[52]

[49] Van der Meulen, N.S., Between Awareness and Ability: Consumers and Financial Identity Theft (March 21, 2011). Communications and Strategies, No. 81, pp. 23-44, 2011. Available at SSRN: http://ssrn.com/abstract=2020214

[50] Meulen, N.S. van der, Lodder, A.R., (2014). Cybersecurity (hoofdstuk 13), in: S. van der Hof, A.R. Lodder, G.J. Zwenne (Ed.), Recht en Computer (6e druk) (pp. 301-318). Deventer: Kluwer.

[51] Origineel: Cybersecurity is het streven naar het voorkomen van gevaar of schade veroorzaakt door storing of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.

[52] Van den Berg, Jan, Van Zoggel, Jacqueline, Snels, Mireille, Van Leeuwen, Mark, Boeke, Sergei, Van de Koppen, Leo, Van der Lubbe, Jan, Van den Berg, Bibi, De Bos, Tony, (2014), On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf

2.2 Wie zijn de Cyber Security Professionals?

In de literatuur zijn veel beschrijvingen gegeven van Cyber Security Professionals. Voordat we de dimensies introduceren waarmee deze professionals in deze arbeidsmarktanalyse worden beschreven, gaan we in op hoe deze professionals in de literatuur worden getypeerd.

'Cybersecurityspecialist' wordt soms als een specifiek beroep aangeduid. De praktijk laat echter iets anders zien. Cybersecurity omvat een breed terrein, met functies variërend van uiterst technisch tot management- en beleidsgeoriënteerd (Burley, 2014).[53] Daar komt bij dat sommige functies in dit veld nog niet uitgekristalliseerd zijn (en dat ook nooit zullen zijn), vanwege de permanente en zeer snelle ontwikkelingen op het terrein van cybersecurity. Verder worden ook zogenoemde 'hybride' of gemengde functies onderscheiden, waarbij verantwoordelijkheden op het gebied van cybersecurity samengaan met andere, vaak niet-gerelateerde, werkrollen (Burley, 2014). 'Dé cybersecurityspecialist' bestaat derhalve niet. Wel kunnen *soorten cybersecurityspecialisten* worden onderscheiden. De literatuur geeft een rijk beeld maar vraagt om nadere structurering.

Er bestaan verschillende inventarisaties en categoriseringen van cybersecurityspecialisten. Zo geeft het 'National Cybersecurity Workforce Framework' (NICE, 2011)[54] een overzicht van het scala aan werkzaamheden, functies, taken en benodigde kennis, vaardigheden en attituden rondom cybersecurity. De gedachte achter dit overzicht is dat taken verschillend over personeel verdeeld kunnen worden.
Het Cyber skills Task Force report (Homeland Security Advisory Council, 2012)[55] onderscheidt een groot aantal soorten cybersecurityfunctionarissen, zoals: systeem- en netwerkpenetratietesters; security-, monitoring- en eventanalisten; intelligence-analisten; forensische analisten.

Het European e-Competence Framework 3.0 (CEN Workshop on ICT Skills, 2014)[56] volgt eenzelfde methode als het Workforce Framework door zich te richten op vijf competentiegebieden ofwel 'e-competence-areas' (Plan, Build, Run, Enable, Manage). Daarbij worden bij elk competentiegebied de bijbehorende specifieke competenties ofwel 'e-competences' aangeduid. Dit framework behandelt niet alleen cybersecurity, maar gaat over ICT in de brede zin.

Tenslotte maakt het beroepsprofiel voor professionals in de informatiebeveiliging (Spruit en Van Noord, 2014)[57] een indeling op basis van het onderscheid tussen enerzijds niveau van handelen (strategisch en/of tactisch en tactisch en/of operationeel) en anderzijds het domein van handelen (domein 'Information risk management' en domein 'ICT security'). Op basis van deze twee onderscheidingen zijn vier specifieke beroepsprofielen voor informatiebeveiligers in kaart gebracht.[58]

---

[53] Burley, D.L., Jon Eisenberg, and Seymour E. Goodman (2014). Would cybersecurity professionalization help address the cybersecurity crisis?: Evaluating the trade-offs involved in cybersecurity professionalization. In: Communications of the acm, Vol. 57, no. 2 Homeland Security Advisory Council. Cyber Skills Task Force Report. Department of Homeland Security, Washington, D.C.
[54] National Initiative for Cybersecurity Education (NICE) (2011). National cybersecurity workforce framework. Retrieved from: http://csrc.nist.gov/nice/framework/
[55] Homeland Security Advisory Council (Fall 2012). Cyberskills Task Force Report.
[56] CEN Workshop on ICT Skills (2014). European e-Competence Framework 3.0. Retrieved from: http://profiletool.ecompetences.eu. Er is ook een Nederlandse versie 2.0 (uit 2010) van dit framework beschikbaar: Europees e-Competence Framework 2.0: http://www.ecompetences.eu/site/objects/download/5228_eCFversie162341NPRCWA2010def.pdf
[57] Spruit, M. en F. van Noord (2014). Beroepsprofielen Informatiebeveiliging. In opdracht van PvIB en QIS.
[58] Namelijk: Chief Information Security Officer (CISO); ICT-beveiligingsmanager; Information Security Officer (ISO); ICT-beveiligingsspecialist. De twee beroepsprofielen in het domein 'ICT security' zijn gebaseerd op het Europees e-Competence Framework 3.0 (en deels aangepast). De twee beroepsprofielen in het domein 'Information risk management' zijn in het onderzoek zelf ontwikkeld, analoog aan de beroepsprofielen uit het domein 'ICT security'.

In navolging van de hiervoor besproken bronnen, wordt ook in dit onderzoek vertrokken vanuit dimensies om tot een zinvolle indeling van functies te komen waarmee de arbeidsmarkt kan worden beschreven. In de literatuur zien we een drietal dimensies terugkomen die van invloed zijn op de inhoud van verschillende functies die als Cyber Security Professional kunnen worden omschreven:

1) De werkzaamheden kunnen als *technisch dominant of niet technisch dominant* gekarakteriseerd worden. Hieraan gerelateerd is het perspectief dat een technische dominante functie een meer ICT-gericht perspectief heeft en een niet technische dominante functie meer gericht is op de organisatie. Dit onderscheid heeft tevens te maken met de kennisclusters die van toepassing zijn bij de verschillende beroepsprofielen. De beroepsprofielen rondom cybersecurity kunnen geworteld zijn in verschillende kennisclusters. Kennisclusters betreffen 'vakgebieden' waaruit bij het werk geput wordt, niet de opleiding(en) die de betreffende CSP gevolgd moet hebben.[59]
2) De functie kan *specifiek gericht zijn op cybersecurity, of cybersecurity als onderdeel hebben*. Dit laatste kan het geval zijn wanneer een professional die werkzaam is een niet-cybersecurityfunctie een deelverantwoordelijkheid krijgt op het gebied van cybersecurity.
3) De functie kan *operationeel-tactisch of tactisch-strategisch* georiënteerd zijn. Het gaat hierbij nadrukkelijk om de aard van de werkzaamheden, niet om het opleidingsniveau van de betrokkene. Een vergelijkbare indeling in strategisch-tactisch-operationeel wordt bij veel werkvelden in o.a. de crisisbeheersing en rampenbestrijding toegepast. Ook in een onderzoek naar vraag en aanbod op de Nederlandse ICT-arbeidsmarkt (Gillebaard, 2014)[60] en het eerder genoemde onderzoek van Spruit en Van Noord naar beroepsprofielen voor de informatiebeveiliging (2014) wordt een vergelijkbare onderverdeling gemaakt.

Op basis van deze dimensies kunnen vier groepen van functies worden onderscheiden, namelijk[61]:

1) *Technisch dominante specialistische cybersecurityfuncties.* Dit zijn beroepen die zeer specifiek op IT/informatiebeveiliging gericht zijn met een hoog-technische component. Tevens kan het gaan om aansturende functies, waarbij een hoog-technische achtergrond vereist is. Het gaat hierbij om functies zoals ethical hacker, penetratie-testers, software testers en technical security engineer
2) *Niet technisch dominante specialistische cybersecurityfuncties.* Hierbij gaat het om cybersecurityspecialisten die meer vanuit een organisatieperspectief naar security kijken. Hierbij onderscheiden we verschillende beroepen en functienamen, zoals

[59] Hierbij kan het gaan om: a) kennisclusters rondom technologie: Techniek; Informatica; MCI (mens-computerinteractie, ook wel aangeduid als MMI: mens-machine-interactie); b) kennisclusters rondom gedrag en handelen: Criminologie; overige gedragswetenschappen (psychologie, communicatiewetenschappen); Ethiek; c) kennisclusters rondom bestuur en maatschappij: Bestuurskunde; Management; Economie; Recht; d) multidisciplinaire kennisclusters: Veiligheidskunde (incl. crisismanagement); e) overig: Sectorspecifieke kennis; Transversale kennis en attitudes.

[60] Gillebaard, H. et al (2014). Dé ICT'er bestaat niet: analyse van vraag en aanbod op de Nederlandse ICT-arbeidsmarkt. Van: DIALOGIC Innovatie - interactie; in opdracht van ECP, Nederland ICT, CIO Platform Nederland.

[61] Dit onderscheid in groepen functies van Cyber Security Professionals is in lijn met het onderscheid dat Professor Jan van den Berg (Van den Berg, Jan, Van Zoggel, Jacqueline, Snels, Mireille, Van Leeuwen, Mark, Boeke, Sergei, Van de Koppen, Leo, Van der Lubbe, Jan, Van den Berg, Bibi, De Bos, Tony, (2014), On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security) maakt tussen de volgende drie typen of 'lagen' van werkvelden binnen cybersecurity: 1) Technologie: dit betreft het puur technische werk, waarbij ICT en cybersecurity in de kern van de werkzaamheden staan; 2) Socio-techniek: dit betreft de interactie van mensen met ICT, waarbij de kern van de werkzaamheden strikt genomen buiten ICT en cybersecurity ligt, maar waarin ICT- en cybersystemen wel een grote rol spelen. In een onderzoek naar beroepsprofielen voor professionals in de informatiebeveiliging (Spruit, M. en F. van Noord (2014). Beroepsprofielen Informatiebeveiliging. In opdracht van PvIB en QIS.) wordt dit type werkveld aangeduid als 'ICT security'. 3) Beleid: dit betreft onder andere management, ethiek, economie, recht en regelgeving, waarbij men bij de werkzaamheden wel oog moet hebben voor ICT en cybersecurity. In het onderzoek van Spruit en Van Noord (2014) wordt bij dit type werkveld gesproken van 'Information risk management'. Een CSP voert zijn werkzaamheden uit in één of meer van deze typen werkvelden. Een onderlinge afstemming en communicatie tussen de verschillende lagen is van belang voor een effectieve cybersecurity.

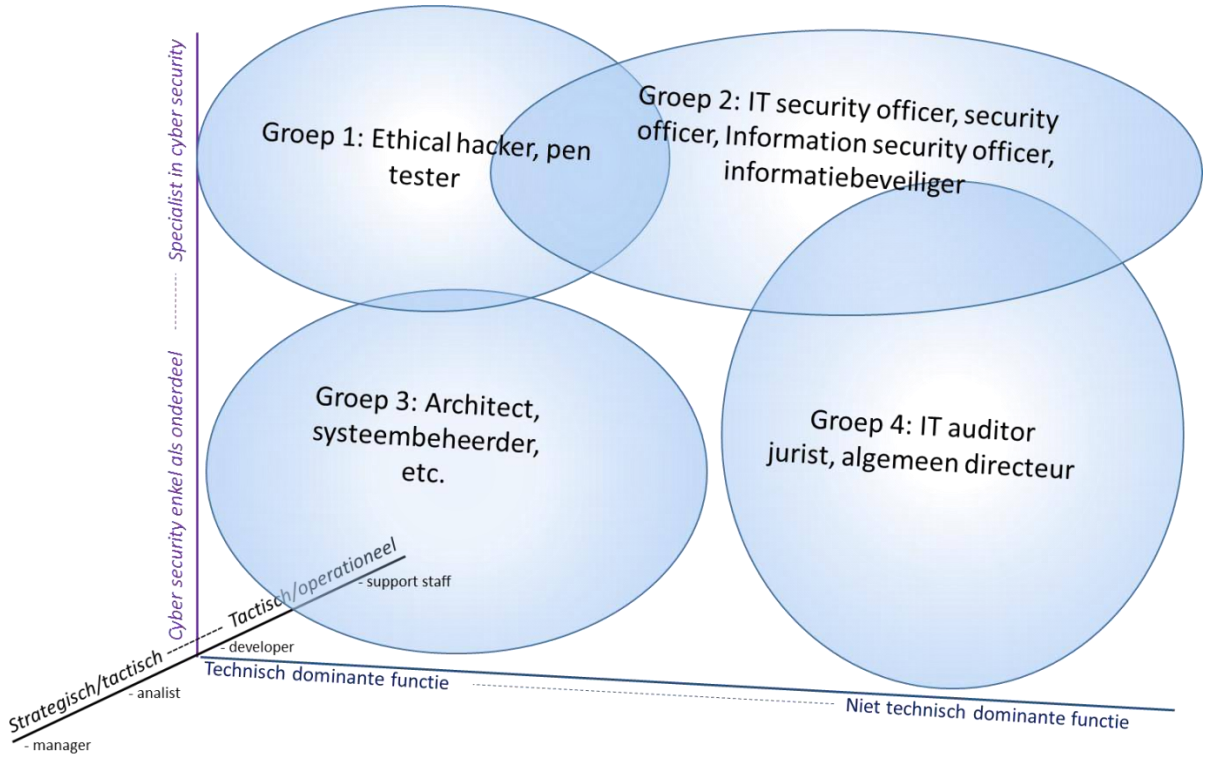
IT security officer, IT security specialist, security officer, Information security officer, informatiebeveiliger.

3) *Technisch dominante functies waarbij cybersecurity een onderdeel is.* Dit zijn beroepen die wel technisch van aard zijn, maar niet gespecialiseerd zijn in cybersecurity. Het gaat hierbij om een brede groep beroepen waarvoor veelal een cybersecurity-gerelateerd certificaat vereist is of als pré wordt aangemerkt. De eerstgenoemde groep (technisch dominante specialistische functies) laten we hierbij buiten beschouwing. Voorbeelden van functies zijn: systeembeheerders, softwareontwikkelaars en architects.
4) *Niet technisch dominante functies waarbij cybersecurity een onderdeel is*, of waarin cybersecurity onderwerp van de kernactiviteit is (bijvoorbeeld jurist in privacy issues, beleidsmedewerker op het gebeid van cybersecurity). Hierbij gaat het dus om onder anderen juristen, algemeen directeuren en auditors. Het gaat om functies waarin cyber eerder als object van een ander domein wordt gezien (bijvoorbeeld object van beleid, rechtspraak) dan als kern van de werkzaamheden.

Daarnaast zijn er functies die minder goed gepositioneerd kunnen worden binnen dit kader, zoals docenten in internetbeveiliging en cybersecurity en onderzoekers (PhDs) die op dit thema werken.

Ten aanzien van de vier functiegroepen moet worden opgemerkt dat deze niet strikt van elkaar te onderscheiden zijn. De invulling van een functie is mede afhankelijk van de organisatie waarin de functie zich bevindt. In grotere organisaties zijn bijvoorbeeld meer mogelijkheden om te differentiëren in functies met een strikter onderscheid tussen de vier functiegroepen. In kleinere organisaties kunnen de vier functies door één persoon worden uitgevoerd. In onderstaand figuur staan de vier groepen en hun onderlinge verhouding schematisch weergegeven.

Figuur 1: Schematisch overzicht functies geïdentificeerd op de arbeidsmarkt



De derde dimensie (niveau van handelen: operationeel-tactisch of tactisch-strategisch) kan binnen iedere functiegroep onderscheiden worden.

2.3 Karakteristieken onderwijs en opleiding

Opleidingen kunnen opleiden tot integrale functies, maar in het aanbod zien we ook veel opleidingen, cursussen en andere vormen van aanbod die veeleer voorbereiden op deeltaken, rollen of werkprocedures die bij functies horen. Hieronder staan enkele karakteristieken van de cybersecurity-opleidingswereld:

- *Certificaten spelen een belangrijke rol in de arbeidsmarkt van CSP's*: Veel ICT-professionals vullen hun formele graad op het gebied van bijvoorbeeld informatica of informatietechnologie aan met zeer gespecialiseerde trainingen waarvoor een certificaat behaald kan worden (Gabberty, 2013).[62]
- *Initiële opleidingen lijken ongeschikt om de benodigde competenties te leveren*: Spruit en Van Noord (2014) geven aan, dat initiële WO- en HBO-opleidingen in het algemeen niet geschikt zullen zijn om direct alle benodigde competenties voor de cybersecurityprofielen op strategisch-tactisch niveau te verwerven. Deze opleidingen kunnen wel het fundament leggen, maar daarna moet men door werkervaring en/of extra cursussen aanvullende competenties verwerven.
- *Niet één route naar het beroep*: De Homeland Security Advisory Council geeft aan dat er een veelheid van wegen bewandeld moet worden om de juiste hoeveelheid mensen op het juiste niveau van voorbereiding te brengen. Genoemd worden: initiële scholing, gerichte opleidingsprogramma's, on the job training, scholing van alumni en veteranen, talentontwikkeling, leren op de werkplek, aanscherping van wervings- en selectiecriteria, en maatschappelijke maatregelen als cybercompetities en banenplannen (Homeland Security Advisory Council, 2012).

Gegeven deze karakteristieken focussen we bij het inventariseren van de soorten opleidingsaanbod op opleidingen gericht op specialisten. Het onderscheid tussen 'specialist' en 'cybersecurity als onderdeel' laten we hierbij buiten beschouwing[63] en de dimensie van handelingsniveau (strategisch tot operationeel) krijgt meer aandacht. We baseren ons hierbij op de categorisering van werkzaamheden van CSP's beschreven in het 'National Cybersecurity Workforce Framework' (NICE, 2011)[64] en de beroepsprofielen voor professionals in de informatiebeveiliging[65]. De hierin opgevoerde werkzaamheden zijn ondergebracht in vier clusters: *managers, analisten*, *developers* en *support staff*. Daarnaast wordt gekeken naar het onderwerp van de werkzaamheden. Hierin sluiten we aan bij het drie ringenmodel van Van den Berg (IT-security, cybersecurity en risicobeleid).[66]

[62] Gabberty, J.W. (2013). Educating the next generation of computer security professionals: the rise and relevance of professional certifications. In: Review of business information systems – Third quarter 2013, volume 17, number 3. Certificaten op het gebied van informatiebeveiliging (Information Assurance) bestaan sinds de late jaren 90. Uit een studie in Maryland blijkt dat in een derde van de vacatures een certificaat gevraagd wordt. De studie onderscheid drie categorieën van populariteit van certificaten. De eerste categorie (CISSP) wordt in duizenden vacatures gevraagd; de tweede categorie (CAP, CISM en SSCP) wordt in honderden vacatures geëist; de laatste categorie (GIAC, ISSEP, GSLC) wordt slechts in enkele tientallen vacatures genoemd (Baltimore Cyber Technology & Innovation Center (CTIC), (2013). Cyber Security Jobs Report).

[63] Dit onderscheid is niet terug te vinden in de opleidingswereld en biedt daarom geen houvast

[64] National Initiative for Cybersecurity Education (NICE) (2011). National cybersecurity workforce framework. Retrieved from: http://csrc.nist.gov/nice/framework/

[65] Spruit, M. en F. van Noord (2014). Beroepsprofielen Informatiebeveiliging. In opdracht van PvIB en QIS.

[66] Van den Berg, Jan, Van Zoggel, Jacqueline, Snels, Mireille, Van Leeuwen, Mark, Boeke, Sergei, Van de Koppen, Leo, Van der Lubbe, Jan, Van den Berg, Bibi, De Bos, Tony, (2014), On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security EducationBerg, J. van den (juli 2014). PPT-presentatie 'Cyber Security Academy (CSA) The Hague: https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf

Figuur 2: Classificatie van opleidingsaanbod naar werkzaamheden en onderwerp van werkzaamheden

Onderwerp ↓	Managers	Analisten	Developers	Support staff
Cyber risicobeleid	Manager cyber risicobeleid	Beleidsmedewerker cyber risicobeleid	Beleidsmedewerker cyber risicobeleid	Support staff cyber risicobeleid
Cybersecurity (cyber risico-inschatting en –beheersing)	Manager cybersecurity	Analist cybersecurity	Developer cybersecurity	Support staff cybersecurity
IT-security (IT risico-inschatting en –beheersing)	Manager IT-security	Analist IT-security	Developer IT-security	Support staff IT-security

In bovenstaand figuur wordt ook de link gelegd met de indeling in functiegroepen. Het onderscheid in niet technisch dominante en technisch dominante functies uit figuur 1 zien we terug in blauwgekleurde cellen van het aanbod (technisch dominant) en het roze deel ervan (niet technisch dominant). Het gebruik van de twee kleuren horizontaal in het midden geeft aan dat hier opnieuw een technisch dominant en een minder technisch dominante deelcomponent bestaat.

Het onderscheid in de linkerhelft van het schema (rood omrand) en het rechter (blauw omrand) betreft een onderscheid in enerzijds meer strategisch tactisch en anderzijds meer tactisch operationele functies. De gebleken indeling in de vacature-analyse (hoofdstuk 3) enerzijds en de analyse van het opleidingsaanbod (hoofdstuk 4) anderzijds laten zich op bovenstaande wijze met elkaar verbinden.

In hoofdstuk 5 worden de arbeidsmarktanalyses en de analyses van het opleidingsaanbod op de hierboven geschetste wijze met elkaar in verband gebracht.

2.4 Discrepanties op de arbeidsmarkt

Vraag en aanbod op de arbeidsmarkt sluiten idealiter naadloos op elkaar aan. Dat is echter in de praktijk (vrijwel) nooit het geval. Op de arbeidsmarkt zijn, op korte en/of (middel)lange termijn[67], globaal gezien drie soorten discrepanties te onderscheiden:

- Van *kwantitatieve discrepanties* is sprake wanneer er voor de cybersecuritysector ofwel te weinig (gediplomeerde) schoolverlaters en andere categorieën werkzoekenden zijn, dan wel er voor deze werkzoekenden (gediplomeerden, werkloze werkzoekenden, baanwisselaars) te weinig vacatures zijn.
- *Kwalitatieve discrepanties* treden op wanneer de technisch-instrumentele eisen en/of sociaal-normatieve eisen van de werkgevers in de cybersecuritysector hoger zijn dan de kennis, kunde, competenties en/of sociale vaardigheden[68] van (gediplomeerde) schoolverlaters en andere categorieën werkzoekenden, dan wel wanneer deze werkzoekenden hogere eisen stellen aan arbeidsinhoud, -voorwaarden en -omstandigheden dan wat werkgevers binnen de sector willen/kunnen bieden.

[67] Ondanks dat voor korte en (middel)lange termijn geen vaste afbakening bestaat, hanteren we de algemeen gebruikte regel dat de korte termijn de verwachting voor één jaar is. De middellange termijn geeft de verwachting weer tot vijf jaar en ten slotte de lange termijn kijkt naar de verwachting over vijf tot tien jaar.
[68] Naar: Van Hoof, J.J. Dronkers, J. (1980). Onderwijs en arbeidsmarkt, een verkenning van de relaties tussen onderwijs, arbeidsmarkt en arbeidssysteem.

- Ten slotte kan sprake zijn van *ondoorzichtigheid (ofwel intransparantie)* van de arbeidsmarkt van de cybersecuritysector. Dan gaat het vooral om verschillen tussen het wervingsgedrag van de werkgevers en het zoekgedrag van (gediplomeerde) schoolverlaters en andere categorieën werkzoekenden. Het kan hierbij zowel gaan om wervingsprocessen van werkgevers en zoekprocessen van werkzoekenden, als om de mate waarin bepaalde groepen werkzoekenden voor werkgevers in beeld komen. Het imago van de sector en het beroep kan hierbij een rol spelen.

Confrontatie van vraag en aanbod maakt eventuele discrepanties zichtbaar op de sectorale arbeidsmarkt op de korte en/of (middel)lange termijn.
Aan de *vraagkant* kijken we naar de volgende aspecten: type functies; aantallen vacatures; functieomschrijvingen (taken, niveau van handelen); functie-eisen (opleidingseisen, aanvullende certificaten, ervaring); profiel werkgevers/wervers (organisatiegrootte, vestigingsplaats, branche, en type zoals publiek, privaat, consultancy); arbeidsvoorwaarden (dienstverband, salaris); en tenslotte de organisatorische inbedding van de werkzaamheden. Aan de *aanbodkant* kijken we naar: de inhoud van opleidingen en trajecten; aantallen opleidingen; aantallen studenten en uitstroom van studenten; en de relatie met de beroepsprofielen. Door beide kanten met elkaar te vergelijken ontstaat een beeld van kwalitatieve en kwantitatieve discrepanties. Daarnaast kijken we naar intransparanties op de arbeidsmarkt (weten werkgevers de werknemers te vinden, weten werkgevers wat zij moeten vragen, weten werknemers het werk te vinden, wat is het imago van het beroep?).

3 De vraag op de arbeidsmarkt naar Cyber Security Professionals

In het voorgaande hoofdstuk hebben we vanuit een theoretisch oogpunt gereflecteerd op de verschillende functieprofielen die met cybersecurity geassocieerd worden. In dit hoofdstuk kijken we naar de actuele en historische vraag naar Cyber Security Professionals. Hierbij wordt eerst een totaaloverzicht van de vraag gegeven. Daarna wordt nadere informatie gegeven over de vraag per functieprofiel.

3.1 Arbeidsmarkt: overzicht totaal en vergelijking met ICT

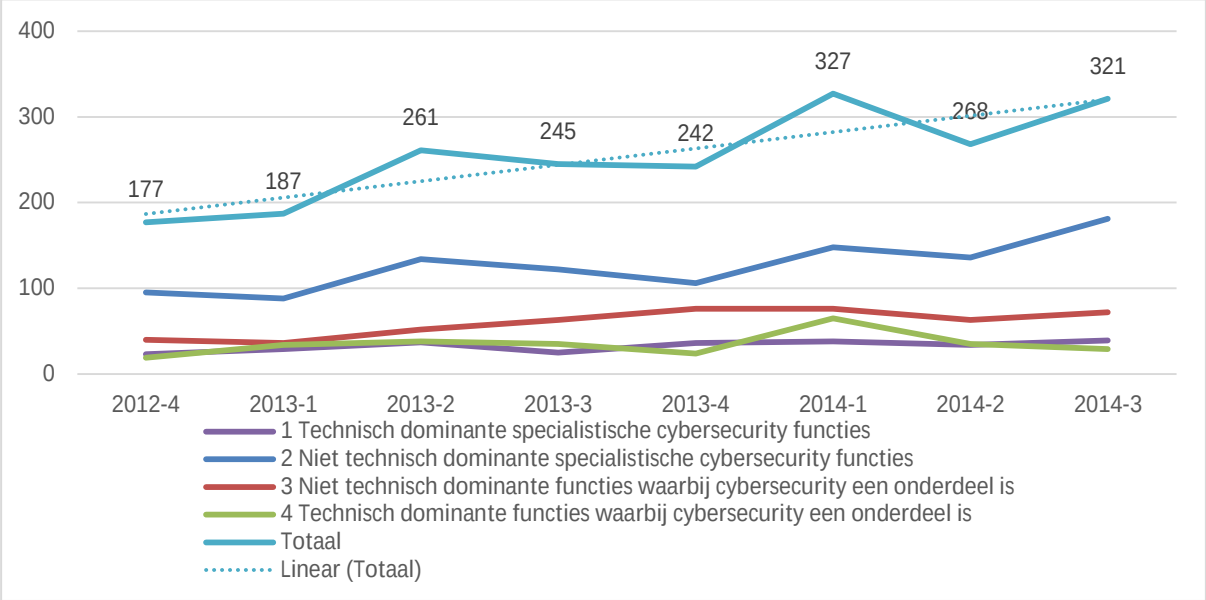
3.1.1 Kwantitatief totaal overzicht

Zoals aangegeven in hoofdstuk 2 (paragraaf 2.2) zijn vier functiegroepen te onderscheiden:

1) Technisch dominante specialistische cybersecurityfuncties.
2) Niet technisch dominante specialistische cybersecurityfuncties.
3) Technisch dominante functies waarbij cybersecurity een onderdeel is.
4) Niet technisch dominante functies waarbij cybersecurity een onderdeel is.

In een periode van zeven kwartalen zijn in totaal ongeveer 2.200 CSP relevante vacatures gepubliceerd[69] (zie voor een toelichting op de gevolgde methode bij de vacatureanalyse, paragraaf 1.5.2.). In onderstaand figuur staat de ontwikkeling van het totaal aantal vacatures en het aantal vacatures per groep weergegeven. Tevens is een trendlijn weergegeven voor het totaal.

Figuur 3: Vraag naar CSP's, uitgesplitst naar technisch dominante en niet technisch dominante-specialistische functies en functies waarin cybersecurity een onderdeel is (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed[70]

[69] Hierbij gaat het unieke vacatures (geen dubbelingen) en niet aangeboden vacatures door intermediairs als uitzendbureaus en headhunters.
[70] Zie hoofdstuk 2 voor methodologische verantwoording.

Gemeten naar het aantal gepubliceerde vacatures in het cybersecuritydomein, is in figuur 3 over de afgelopen zeven kwartalen een toename van de totale vraag naar CSP's waar te nemen. Waar de totale vraag in het laatste kwartaal van 2012 en eerste kwartaal van 2013 nog onder de 200 vacatures lag, piekt deze in het eerste kwartaal en derde kwartaal van 2014 ver boven de 300 vacatures. Interessant is dat de vraag in het tweede kwartaal van 2014 enigszins terugviel tot het niveau van 2013. De sterke stijging in het eerste kwartaal van 2014 is vooral te zien bij de functies 'security officer', 'IT security specialist (beide niet technisch dominante specialist) en 'IT auditor' (technisch dominante functie waarin cybersecurity een onderdeel is). Een eenduidige verklaring van de piek in het eerste kwartaal van 2014 is er niet, maar deze kan liggen in het feit dat door de publiciteit rond cybersecurity-incidenten bedrijven en organisaties zich meer bewust worden van cyberrisico's en er meer nadruk op cybersecurity ligt in audits.[71]

Wat betreft de vraag naar CSP's op jaarbasis waren er in Nederland (gerekend over het laatste kwartaal van 2013 en de eerste drie kwartalen van 2014) 1158 gepubliceerde vacatures in het cybersecuritydomein. In de eerste drie kwartalen van 2014 waren er 916 gepubliceerde vacatures.

Op basis van een vergelijkbare methodiek (als toegepast in dit onderzoek) wordt het aantal in 2013 in de Verenigde Staten geschat op 209.749.[72] Afgezet tegen de totale bevolking worden in Amerika tien keer meer vacatures gepubliceerd. In deze Amerikaanse studie is gekeken naar relevante job-titels, certificaten en cybersecurity-gerelateerde taken. Hiermee is de definitie breder dan die gebruikt in dit onderzoek.

Ten aanzien van het totaal aantal gepubliceerde en getelde vacatures gaat het onderzoeksteam er van uit dat dit aantal een onderschatting is van de totale vraag naar cybersecurity-gerelateerde professionals. De volgende overwegingen spelen hierbij een rol:

- Een deel van de professionals *stroomt direct in vanuit opleiding/stage*. Dit geldt vooral voor de technisch dominante functies waarbij cybersecurity een onderdeel is.
- Een deel stroomt in *via informele wervingskanalen* zonder dat er een vacature gepubliceerd wordt. Hierbij gaat het om 'challenges', maar ook om informele netwerken en aanbrengbonussen. Dit geldt vooral voor de technisch dominante specialistische cybersecurityfuncties.
- Vacatures worden niet gepubliceerd omdat het aangeeft dat de organisatie de security niet op orde heeft (*vacature geeft een zwakte weer*). Dit geldt vooral voor de niet technisch dominante specialistische cybersecurity.
- De vraag komt niet tot uiting in de vacature- en functieomschrijving maar pas in de concrete aanpassing van het *takenpakket*. Dit geldt vooral voor de niet technisch dominante functies waarbij cybersecurity een onderdeel is.

Op basis van de beschikbare gegevens is het niet mogelijk deze onderschatting van de vraag te kwantificeren. We gaan daarom uit van de gepubliceerde vacatures en benoemen waar onderschattingen van de vraag aan de orde zijn.

In de beschrijving van iedere functiegroep (in paragraaf 3.2 tot en met 3.5) komen verschillende aspecten specifieker aan bod, zoals de inhoud van functiebeschrijvingen, historische ontwikkeling van de vraag, kenmerken van werkgevers, functie-eisen en arbeidsvoorwaarden. Daarnaast schetsen we, op basis van de analyse van omgevingsfactoren en interviews met werkgevers en CSP's, de ontwikkeling van de vraag naar specifieke functiegroepen in de toekomst.

[71] Bij deze totalen moet worden opgemerkt dat hierin de jaarlijkse werving van 35 medewerkers van het Team High Tech Crime van de Politie, evenals de werving van Cyber Security Professionals door Defensie, niet zijn meegenomen doordat deze niet als vacatures in Jobfeed zijn opgenomen (de werving vindt plaats door middel van een online challenge).

[72] Zie: Burning Glass (2014), Job Market Intelligence: Report on the Growth of Cybersecurity Jobs

Voordat we ingaan op de vier functiegroepen, schetsen we het bredere kader van de arbeidsmarkt van ICT-professionals. Dit om de vraag naar CSP's te positioneren ten opzichte van de totale vraag binnen de ICT en om een oordeel te vellen of de vraag naar CSP's kleiner, groter of vergelijkbaar is met die van ICT-professionals in het algemeen.

3.1.2 Vraag CSP's, **vraag ICT'ers en bepaling totale werkgelegenheid**

Mede als gevolg van de in hoofdstuk 1 beschreven ontwikkelingen is in de ICT in de brede zin sprake van grote veranderingen in beroepen en functies en de daarvoor gevraagde competenties. Meer en meer bestaat behoefte aan HBO en WO-opgeleiden, terwijl het aantal banen op MBO-niveau sterk afneemt. Op de lagere MBO-niveaus is een beweging zichtbaar naar combinatiefuncties waarin ICT een rol speelt (bijvoorbeeld zorgfuncties en beveiligingsfuncties met een ICT-component). Het belang van ICT-kennis in niet-ICT-functies neemt daarmee toe. Door de toename van het aantal gebruikers van ICT-producten en de complexiteit van ICT-producten, ontstaat behoefte aan 'vertalers' van ICT-producten naar gebruikers.[73] Degelijke functies vragen om goede sociale en communicatieve vaardigheden. Tegelijkertijd ontstaan ook nieuwe functies, nauw samenhangend met de technologische ontwikkelingen (zoals big data, cloud computing, 3D printing) en de behoefte meer in te spelen op klantwensen.[74]

Daarnaast zijn in de beroepspraktijk van ICT'ers de volgende meer specifieke trends te signaleren. Onderstaande box vat deze kort samen.

Trends in de beroepspraktijk van ICT'ers[75]*:*

- *Het nieuwe werken: Plaats- en tijdonafhankelijk werken raakt steeds meer ingeburgerd. Voor de werkgever betekent dit onder meer dat minder kantoorwerkplekken nodig zijn. Voor de ICT-helpdesk betekent dit dat deze steeds meer een 'stand-by'-functie op afstand krijgt.*
- *Bring Your Own Device: Steeds meer medewerkers gebruiken tijdens het werk zelf aangeschafte apparaten (smartphone, laptop of tablet). Systeembeheerders dienen alles veilig draaiend te houden. Verder is de tijd van één systeem voorbij. De dominantie van de Windows-PC zal de komende jaren afkalven tot ruwweg de helft van de gebruikte apparatuur. Andere systemen zullen marktaandeel winnen.*
- *Offshoring als uitdaging: Het offshoren van gestandaardiseerde processen en 24/7-diensten naar het buitenland hoeft niet ten koste te gaan van de ICT-werkgelegenheid in Nederland. Het biedt ruimte voor meer inhoudelijke en interessantere functies in Nederland.*
- *Leven lang leren, iedereen digitaal: Door de snelheid van technologische ontwikkelingen is kennis steeds sneller verouderd. Hierdoor bestaat behoefte aan een nieuwe manier van een 'leven lang leren'. Belangrijk onderdeel van de Digitale Agenda van het Ministerie van EZ is het streven naar een digitaal basisniveau voor elke werknemer, door het in het onderwijs aanleren van ICT-vaardigheden en basiskennis. Het bewustzijn van het bedrijfsleven van het belang van voldoende digitale vaardigheden voor iedere werknemer neemt ook toe.*
- *Sociale netwerken: Sociale netwerken (Twitter, LinkedIn, Facebook e.d.) hebben definitief hun intrede gedaan in het marketing- en communicatiebeleid van bedrijven. De grens tussen zakelijk en privé vervaagt daardoor. Steeds meer bedrijven hebben daarom richtlijnen voor het gebruik van social media tijdens het werk.*

3.1.2.a Werkgelegenheid en vacatures in de ICT- en CSP-beroepen

Ondanks dat niet alle CSP's ICT'ers zijn, is het om twee redenen interessant te kijken naar de werkgelegenheid en vacatures in alle ICT-beroepen:

[73] Een voorbeeld is de elektrostylist, die consumenten wegwijs maakt in de domotica (huisautomatisering).
[74] UWV (2014). Sectorbeschrijving Informatie en Communicatie.
[75] Zie: http://www.ecabo.nl/ict-en-media/trends-ontwikkelingen/

- Ten eerste overlapt de arbeidsmarkt voor Cyber Security Professionals voor een behoorlijk deel met die van de rest van de ICT. Het gaat vaak om dezelfde basisopleidingen, terwijl tevens veel ICT'ers inmiddels een klein stukje cybersecurity in hun pakket hebben.
- Ten tweede hebben we geen cijfers over de werkgelegenheid in de cybersecurity. Hieronder vergelijken we de aantallen vacatures van de cybersecurity met die in de hele ICT. Door de vacaturegraad in beide segmenten gelijk te stellen is een schatting te maken van de werkgelegenheid voor Cyber Security Professionals.

3.1.2.b Werkgelegenheid in de ICT-beroepen

Onderstaande tabel laat de werkgelegenheid in ICT-functies naar opleidingsniveau zien. Daarbij is onderscheid gemaakt naar het Rijk, de rest van het ABP-domein (medeoverheden, zbo's, defensie, rechtspraak, politie, brandweer, onderwijs) en de marktsector.

Tabel 1: Verdeling beroepsbevolking per kennisniveau naar sector, 2013

Sector	Rijk	Overig ABP-domein	Markt-sector	Totaal	Rijk	Overig ABP-domein	Markt-sector	Verdeling niveaus ICT
	Aantal x 1.000				Aandeel in %			
ICT/automatisering middelbaar	2,8	12	83,1	97,8	3%	12%	85%	33%
ICT/automatisering hoog	5,2	8,7	148,8	162,7	3%	5%	91%	54%
ICT/automatisering wetenschappelijk	3,1	1,7	35,6	40,4	8%	4%	88%	13%
Totaal ICT/automatisering	11	22,4	267,8	300,9	4%	7%	89%	100%
Alle beroepen (totale beroepsbevolking)	116,3	1.055,7	7.418,0	8.590,1	1%	12%	87%	

Bron: Panteia op basis van P-Direkt en Enquête beroepsbevolking (CBS).

In totaal werkten er in 2013 ruim 300.000 personen in ICT-beroepen. Bij de Rijksoverheid werken in verhouding tot de totale werkgelegenheid relatief veel ICT'ers; dat zijn vervolgens relatief vaak academici. Binnen het totale ABP-domein (rest van de overheid plus onderwijs) is het aandeel ICT'ers laag, maar dat is vooral het geval binnen het onderwijs. In de laatste kolom van de tabel is te zien dat het grootste deel van de ICT'ers (54%) op HBO-niveau werkt en dat het aandeel academici met 13% gering is.

3.1.2.c Ontwikkeling van economie en arbeidsmarkt

In de *Macro Economische Verkenning 2015* voorspelt het Centraal Planbureau (CPB) voor 2015 een zeer matige economische groei van 1,25 procent. Tevens geeft het aan dat er nogal wat risico's spelen waardoor dit groeicijfer ook nog wel eens lager zou kunnen uitvallen. Naast deze meest actuele voorspelling heeft het CPB in de rapportage *Roads to Recovery* ook nog een inschatting gemaakt in hoeverre in de periode 2016-2023 sprake zal zijn van herstel van de door de economische crisis veroorzaakte terugval van de economie. Daarbij meldt het CPB dat alleen in het meest gunstige van de drie scenario's ("Aantrekkend" met een gemiddelde economische groei van 2% per jaar) er sprake zal zijn van een verbetering op de arbeidsmarkt. In de andere twee scenario's blijft de werkloosheid gelijk of neemt deze zelfs toe. Achtergrond is dat de toename van de arbeidsproductiviteit in deze scenario's even groot of zelfs groter is dan de economische groei. Er zijn dan minder werkenden nodig om de economie draaiende te houden. Daarbij spelen ook nog een krimpende overheid en een tijdelijke stabilisering van de werkgelegenheid in zorg en welzijn. Digitalisering is trouwens wel een belangrijke achtergrond voor de toename van de arbeidsproductiviteit. Wanneer arbeidsorganisaties daarop zwaarder inzetten, betekent dat ook dat de vraag naar ICT'ers toeneemt.[76]

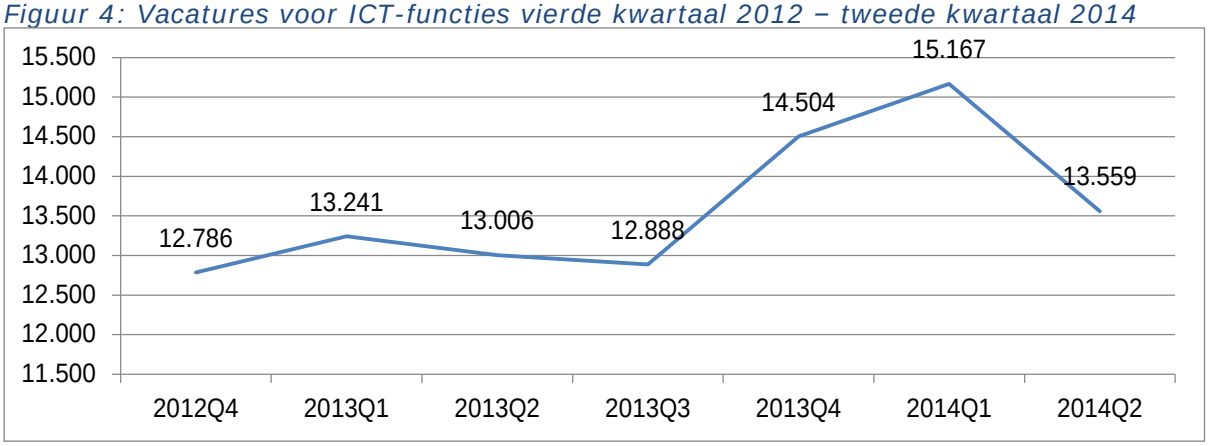
[76] Gek genoeg zit het aspect dat de hogere arbeidsproductiviteit tot minder vraag op de arbeidsmarkt leidt en dat daarvoor dan vervolgens meer ICT-ers nodig zijn, vaak niet in de modellen die de toekomstige vraag naar ICT-ers berekenen. Dit is trouwens wel het geval in de recente *Arbeidsmarktanalyse Rijk* van Panteia en Ecorys.

De vraag naar ICT'ers wordt ook door andere dan economische ontwikkelingen beïnvloed. Belangrijk is de trend van "extrapolisering" van de arbeidsmarkt. Alle prognoses duiden erop dat de vraag naar hoger en lager opgeleiden stijgt, terwijl die naar middelbaar opgeleiden daalt. Achtergronden zijn verplaatsing van arbeid naar lage lonen landen en opnieuw de digitalisering. Dit is een eerste oorzaak voor het krapper worden van de arbeidsmarkt op HBO- en WO-niveau. Uit de *Arbeidsmarktanalyse Rijk* van Panteia en Ecorys (2014) komt dan ook een toenemende krapte aan ICT'ers op HBO- en WO-niveau naar voren. Daarbij komt ook nog dat arbeidsorganisaties meer waarde hechten aan sociale competenties (communicatief, teamwork, leiding geven, verantwoordelijkheid nemen, etc.) van die hoger opgeleiden, in het bijzonder de HBO'ers. Dat geldt voor alle sectoren. Voor veel functies binnen de cybersecurity zijn die sociale competenties ook van belang. Werkgevers krijgen voor de betreffende functies in de toekomst te maken met nog meer concurrentie op de arbeidsmarkt dan er nu al is.

3.1.2.d Vacatures voor ICT-beroepen

De volgende figuur laat het aantal vacatures voor ICT-functies over de afgelopen twee jaar zien.

Figuur 4: Vacatures voor ICT-functies vierde kwartaal 2012 – tweede kwartaal 2014



Bron: Panteia/PLATO op basis van vacature-analyse Jobfeed

Tot en met het derde kwartaal van 2013 lag het aantal vacatures voor ICT'ers redelijk stabiel op ongeveer 13.000 vacatures per kwartaal. Daarna was een flinke stijging zien, tot meer dan 15.000 vacatures in het eerste kwartaal van 2014. Zoals figuur 3 (Vraag naar CSP's) laat zien, is eenzelfde, maar minder uitgesproken piek te zien met betrekking tot de vacatures voor Cyber Security Professionals, namelijk een stijging van 242 in het vierde kwartaal van 2013 naar 327 in het eerste kwartaal van 2014). In het tweede kwartaal van 2014 neemt het aantal vacatures voor ICT'ers weer af, hoewel het nog steeds wat boven het eerdere niveau ligt. Als we over deze hele periode het jaarlijkse aantal vacatures afzetten tegen het aantal werkenden, dan is het aantal werkenden bijna zesmaal het aantal vacatures.

3.1.2.e Toekomstige aansluiting op de arbeidsmarkt in de ICT (en cybersecurity)

Om te bepalen wat de vraag naar ICT'ers is op de middellange termijn (2017-8), zijn diverse onderzoeken uitgevoerd. De belangrijkste daarvan zijn van het ROA (De arbeidsmarkt naar opleiding en beroep, 2013), Etil (Arbeidsmarkt ECABO-domein 2013-2018, 2014) en Panteia (Arbeidsmarktanalyse Rijk, 2014). De tekstbox hieronder geeft weer hoe verschillende bronnen de vraag naar ICT'ers in de toekomst duiden.

ROA doet geen afzonderlijke uitspraken over de ICT-sector, maar stelt wel dat de vervangingsvraag van informaticaberoepen voor 99% bepalend is voor de vraag op de ar-

beidsmarkt (er is amper uitbreidingsvraag vanwege nieuwe of uitbreidende bedrijfsactiviteiten) en dat de vervangingsvraag voor informaticaberoepen de komende periode met 40% zal afnemen. Dat duidt op weinig krapte op de arbeidsmarkt aangezien het aantal studenten niet afneemt. ROA doet deze uitspraken grotendeels op basis van trendanalyses: hierin is bijvoorbeeld niet meegenomen dat de vraag naar informaticafuncties verandert (upgrading of vraag naar cybersecurity), terwijl werkenden in de informatica op alle niveaus betreft. Ook is niet gerekend met een toename van digitalisering/robotisering.

Etil schat de kansen van MBO-gediplomeerden in de ICT om aan werk te komen voor de lagere MBO-niveaus laag in. Het perspectief begint echter beter te worden naarmate het opleidingsniveau hoger wordt. Voor netwerkbeheerders niveau 4 is het perspectief in sommige regio's zelf erg gunstig. Dat betekent data werkgevers moeilijker aan personeel kunnen komen. Etil doet geen uitspraken over HBO'ers.

Panteia houdt in de inschatting van de arbeidsmarkt voor ICT'ers in 2017 en 2020 rekening met twee factoren die zijn vastgesteld in gesprekken met HR-functionarissen bij het Rijk: 1. De digitalisering neemt toe en 2. de vraag naar HBO-opgeleide ICT'ers met goede sociale vaardigheden neemt toe. Mede als gevolg hiervan komt Panteia tot de conclusie dat er in 2017 een tekort aan op HBO-niveau opgeleide ICT'ers ontstaat. In 2020 zou dit ook gaan gelden voor het (hogere) MBO-segment. Op de laagste niveaus zullen grote overschotten ontstaan.

Omdat voor de cybersecurity juist (sociaalvaardige) HBO'ers (en soms MBO-4 opgeleiden) nodig zijn, lijkt een scenario van krapte voor dit segment van de ICT het meest waarschijnlijk. De huidige constatering van werkgevers dat men moeilijk aan personeel kan komen bevestigt dit ook. De Intelligence Group meldt dat 44% van de ICT'ers maandelijks wordt benaderd door een recruiter (ICT-arbeidsmarktmonitor 2014)[77].

3.1.2.f Werkgelegenheid in CSP-beroepen

Als de verhouding vacatures staat tot werkgelegenheid van CSP's gelijk is aan die van de rest van het ICT-personeel (namelijk 1: 6),[78] dan zou de omvang van de werkgelegenheid aan CSP's dit jaar naar schatting op ruim 7.000 personen liggen.
Het gaat hier overigens vooral om mannen. Er zijn redenen om aan te nemen dat het relatieve aantal vacatures voor CSP's hoger ligt dan dat voor ICT'ers in het algemeen. De toegenomen beleidsaandacht en urgentie om aandacht te besteden aan cybersecurity doen vooral het aantal CSP's sneller groeien. Een mogelijke oorzaak is ook gelegen in het gegeven dat de vergrijzing van de beroepsgroep CSP's minder is dan die van ICT'ers in het algemeen. Dat leidt tot een kleinere vervangingsvraag vanwege pensioen en ziekte e.d.[79]

Als de verhouding vacatures staat tot werkgelegenheid anders ligt dan hierboven gesteld (namelijk vergelijkbaar met de verhouding tussen vacatures en werkgelegenheid van ICT- personeel), dan verandert ook de schatting van de werkgelegenheid op basis van het vastgestelde aantal vacatures. Als er bijvoorbeeld in verhouding tot ICT-personeel meer CSP vacatures zouden zijn ten opzichte van de werkgelegenheid, dan zou de totale

[77] Zie: http://www.intelligence-group.nl/nl/actueel/downloads/ict-arbeidsmarktmonitor-2014#collapseForm
[78] In 2013 was de totale werkgelegenheid in de ICT/automatisering ongeveer 300.000 (zie tabel 1; bron: Panteia op basis van P-Direkt en Enquête beroepsbevolking (CBS)). Het totaal aantal vacatures op jaarbasis is ongeveer 50.000 (zie figuur 4; bron: Panteia/PLATO op basis van vacatureanalyse Jobfeed). De verhouding tussen het aantal vacatures en de totale werkgelegenheid is daarom 1 : 6.
[79] De vraag die tot uiting komt in vacatures kan betrekking hebben op een vervangingsvraag (medewerkers bereiken de pensioengerechtigde leeftijd) en een uitbreidingsvraag (er zijn in totaal meer professionals nodig). Gegeven dat cybersecurity een relatief jong vakgebied is, is de verwachting dat de vervangingsvraag geen grote rol speelt (er gaan weinig professionals met pensioen) en dat de toename in de vraag volledig verklaard kan worden door de uitbreidingsvraag.

werkgelegenheid voor CSP's lager uitvallen (als de verhouding 1: 5 zou zijn, dan is de totale werkgelegenheid CSP's 6.000).

Zoals aangegeven, komt in de volgende vier paragrafen (3.2 tot 3.5) de vraag naar de verschillende functiegroepen van CSP's aan de orde.

3.2 Arbeidsmarkt voor technisch dominante specialistische cybersecurityfuncties (functiegroep 1)

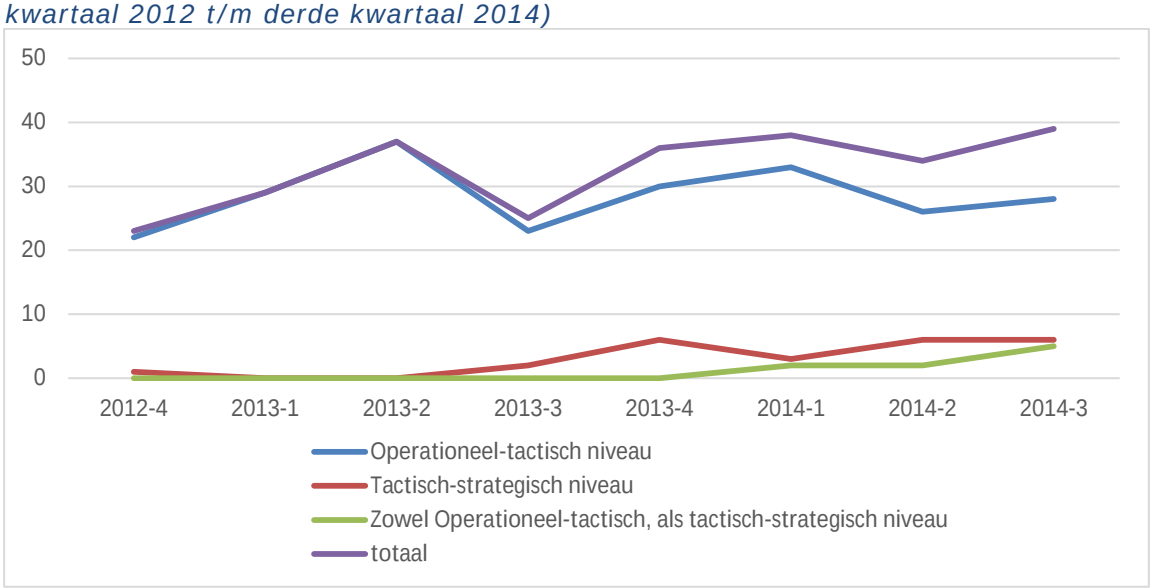
In de vacature-analyse is een aantal functies geïdentificeerd die als technische dominante cybersecurityspecialisten kunnen worden gekarakteriseerd. Hierbij gaat het om functies die vooral operationeel-tactisch zijn, maar er is ook een aantal functies op tactisch/strategisch niveau geïdentificeerd. Binnen dit domein komen we de volgende functies/omschrijvingen tegen op de verschillende niveaus:

- *Operationeel-tactisch niveau* (tester software, informaticus, information engineer, ethical hacker, pen tester, consultant).
- *Tactisch-strategisch niveau* (hoofd informatievoorziening, accountmanager IT, manager, Coördinator informatiebeveiliging, Manager New Technology & Security).
- *Zowel Operationeel-tactisch, als tactisch-strategisch niveau* (beveiligingsspecialist, teamleider software testing, veiligheidskundige).

3.2.1 Kwantitatief overzicht vacatures (aantallen en historisch overzicht)

Totaal waren er de afgelopen zeven kwartalen ongeveer 260 vacatures voor functiegroep 1. Bijna 90% (87%) van de vacatures was voor functies die als operationeel-tactisch gekenmerkt worden; ongeveer 9% ging om functies op tactisch-strategisch niveau, en 3% bestaat uit functies op zowel operationeel-tactisch als tactisch-strategisch niveau. Onderstaande figuur geeft de ontwikkeling van de vraag naar de verschillende functies op de genoemde niveaus weer over zeven kwartalen (vierde kwartaal 2012 t/m derde kwartaal 2014).

Figuur 5: Vraag naar technisch dominante specialistische cybersecurityfuncties (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

Door de tijd heen is een lichte toename van de totale vraag naar technische dominante specialisten te zien. In het laatste kwartaal van 2012 werden ongeveer 25 vacatures ge-

publiceerd, in het laatste kwartaal van 2013 en de drie kwartalen van 2014 waren er ongeveer 35-40 vacatures. Echter, opgemerkt moet worden dat het aantal gepubliceerde vacatures waarschijnlijk een onderschatting is van de totale vraag. Met betrekking tot deze groep wordt gebruik gemaakt van alternatieve wervingskanalen zoals informele (professionele, hackers) netwerken en contacten, en hackers challenges. Ook hebben organisaties standaard een open vacature online staan voor dit type functies.

3.2.2 Functiebeschrijvingen

Als we naar de functieomschrijvingen kijken komen we de volgende kerntaken tegen binnen de technisch dominante specialistische cybersecurityfuncties:

- *Onderzoeken/testen*: veel functies zijn gericht op het opsporen van veiligheidslekken en het afhandelen van security-incidenten. Daarnaast vragen veel vacureteksten om een onderzoekende houding in het analyseren van risico's, kwetsbaarheden en afhankelijkheden. In de meer tactisch-strategische functies komt naar voren dat de CSP in staat moet zijn onderzoeken te begeleiden en te laten uitvoeren. Onderzoeksprojecten en opdrachten kunnen liggen op het terrein van beveiliging van netwerken, ethical hacking, integriteit van software, identity management, business continuity management, infrastructuurbeveiliging, en privacy en security.
- *Bouwen*: taken zoals ontwerpen, bouwen en aanpassen van complexe IT-securitysystemen komen regelmatig voor in de functieomschrijvingen.

Hieronder staat een tweetal voorbeelden van functiebeschrijvingen.

Als Certified Ethical Hacker ga je op ethische wijze op zoek naar zwakheden in het netwerk, de producten en diensten. Je gebruikt je expertise, kennis en ervaring om onderzoek te doen naar de zwakke plekken van de organisatie. Je verzorgt documentatie en zorgt voor een rapportage met advies voor verbetering van de security. Je doet penetratietests en test kwetsbaarheden volgens de marktgeaccepteerde methodes en protocollen.

Als Technical Consultant Security ontwerp, bouw en review je complexe IT-security-oplossingen bij onze (internationale) klanten. Je ontwerpt technische oplossingen, denkt mee en adviseert hoe security het beste kan worden benut binnen de bedrijfsprocessen van de klant. Je inventariseert aan welke eisen een security-oplossing moet voldoen en adviseert onze klanten met welke oplossingen zij het efficiëntst kunnen werken.

3.2.3 Functie-eisen: opleidingsniveau en competenties

Naast de omvang van het aantal vacatures geven de vacatures ook informatie over de functie-eisen. Hierbij kijken we naar het totale aantal vacatures over de laatste zeven kwartalen. Zo blijkt met betrekking tot het gevraagde werk- en denkniveau uit de vacature-analyse dat in 26% van de vacatures een WO-niveau wordt gevraagd, 26% vraagt een HBO-/WO-niveau, 38% vraagt een HBO- werk- en denkniveau en 5% vraagt om een MBO-/HBO-niveau. Ondanks dat voor tactisch-strategische functies vaker een WO-niveau wordt gevraagd dan voor functies op operationeel-tactisch niveau (42% ten opzichte van 24%) is ook dit laatste percentage hoog te noemen. Een mogelijke verklaring hiervoor is dat veel operationele functies zeer specialistisch zijn en daarom een hoog denk- en werkniveau vereisen. Interessant is, dat in een aantal gevallen expliciet vermeld wordt, dat de opleidingseis niet keihard is (zie voorbeeld hieronder).

Let op: heb je een andere MBO-, HBO- of WO-opleiding maar wel bijzonder veel (aantoonbare) affiniteit met security, ook dan ben je welkom in ons ICT Security Traineeship. Ook als je al enkele jaren werkervaring hebt (maximaal 3 jaar) dan nodigen wij je van harte uit om te solliciteren!

Naast het opleidingsniveau staan ook functie-eisen beschreven in de vacatures. De functie-eisen zijn vanzelfsprekend gerelateerd aan de functieomschrijving. Veel voorkomende eisen zijn:

- *Specialistische IT-kennis*, zoals kennis van internet en computernetwerken. Veel vacatures specificeren de vereiste kennis van programmatuur, talen, standaarden en pakketten.
- *Kennis van IT-dreigingen*: kennis van dreigingen en risico's met betrekking tot computernetwerken en van maatregelen die je daartegen kunt nemen wordt als zeer belangrijk ervaren.
- *Adviseren*: de specialisten moeten in staat zijn organisaties (intern/extern) te adviseren over IT-oplossingen op securitygebied.
- *Andere vereiste attitudes* zijn initiatiefrijk, samenwerken, resultaatgericht, onderzoeks-minded, omgevingssensitiviteit, begrip van ethisch handelen.
- *Ervaring*: veel vacatures vragen om minimaal 3 jaar ervaring. Ondanks dat het overgrote deel vraagt om meer ervaring, is er ook een aantal vacatures voor starters. Ook worden traineeships aangeboden.

Opleidingseisen zijn niet altijd in de vacaturetekst gespecificeerd. Vaak wordt een technische opleiding of in ieder geval affiniteit met techniek verondersteld. Wat betreft ervaringseisen kan het gaan om hobbyistische ervaring in programmeren en hacken.

Hieronder is een voorbeeld weergegeven van een typische omschrijving van de functie-eisen.

Tester software […]
Functie eisen:
- *Je hebt begrip van ethiek en een sterk gevoel voor ethiek in bedrijfsvoering en informatiebeveiliging en respecteert deze;*
- *Je hebt een afgeronde HBO-/WO-opleiding, minimaal 3 jaar relevante werkervaring, aangevuld met OSCP/ OSCE/ CEH, of gelijkwaardig gecertificeerd, of aantoonbaar zeer grote vaardigheid in hacking(contests);*
- *Je hebt aantoonbare kennis van ICT, -architecturen, -netwerkinfrastructuren, -systemen, -applicaties, -(web)portals en securitycomponenten zoals firewalls, IDP/S, en encryptie technologieën;*
- *Je bent klant- en servicegericht en in het bezit van goede communicatieve vaardigheden om kwetsbaarheden uit te leggen;*
- *Je kunt aantoonbaar kwetsbaarheden vinden, aantonen en rapporteren; Je combineert theoretische kennis met hands-on ervaring; Je hebt gevoel voor techniek, bedrijfsvoering en security;*
- *Je bent analytisch en kunt zelfstandig overzicht houden bij complexe storingen en uitdagingen en weet daartoe flexibel en oplossend te handelen;*
- *Je stelt vragen, bent nieuwsgierig en creatief, je bezit een CAN-DO-LET'S-DO mentaliteit.*

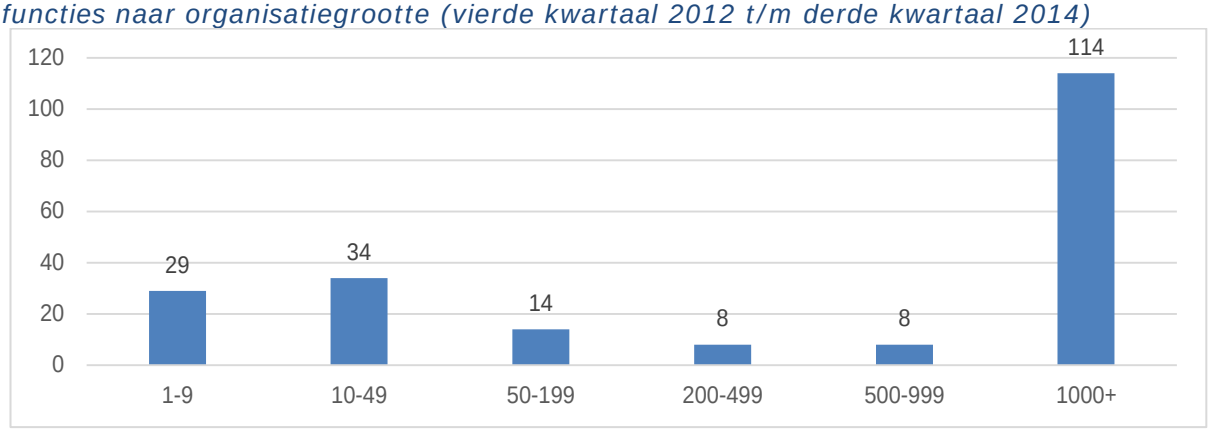
Pré's en wensen:
- *Je hebt een CISSP, of vergelijkbare technische securitycertificering.*
- *Je wilt je graag ontwikkelen door meerdere internationaal erkende securitycertificeringen te blijven behalen.*

De startersfuncties en traineeships zijn vooral te vinden bij de consultancy- en detacheringsbedrijven. Ervaren Cyber Security Professionals hebben vaak een achtergrond in de consultancy voordat zij verantwoordelijk worden voor het ICT-beveiligingsbeleid bij een organisatie. De consultancy- en detacheringsbedrijven vervullen daarom een opleidingsfunctie op het gebied van cybersecurity. Hierbij moet worden opgemerkt dat de starters door consultancy- en detacheringsbedrijven bij organisaties worden ingezet waardoor de organisaties ook investeren in de kennisontwikkeling van starters.

3.2.4 Profiel werkgevers

De technisch dominante specialistische cybersecurityfuncties worden voornamelijk gevraagd binnen de ICT (40%), zakelijke dienstverlening (13%), financiële dienstverlening, banken en verzekeraars (6%), en overheid (4%). Voorbeelden van organisaties die veel vacatures hebben gepubliceerd zijn Sogeti, KPN, PwC, Deloitte, Ziggo, Philips, Ministerie van Defensie en ING[80]. Echter, aangezien de challenges van de Politie (35 vacatures per jaar) en Defensie (werven ongeveer 30 professionals in 2014) niet in het vacatureoverzicht zijn opgenomen, kan het beeld van de vraag m.b.t. deze professionals enigszins vertekend zijn. In onderstaande figuur is de verdeling van vacatures naar organisatiegrootte weergegeven.

Figuur 6: Totaal aantal vacatures voor technisch dominante specialistische cybersecurityfuncties naar organisatiegrootte (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

Uit bovenstaande figuur, en het overzicht van grote wervers, blijkt dat het vooral de grote organisaties zijn die vacatures voor cybersecurityspecialisten te vervullen hebben. Zij zijn verantwoordelijk voor een derde van de totale vraag.

3.2.5 Arbeidsvoorwaarden

Ten slotte geeft de vacature-analyse informatie over het voorziene dienstverband. Meer dan 80% van de vacatures stelt een fulltime dienstverband (>32 uur) in het vooruitzicht, 9% geeft aan dat zowel fulltime als parttime een optie is. In 12% van de vacatures gaat het om een dienstverband van minder dan 32 uur. In vergelijking met de arbeidsmarkt in het algemeen is er weinig vraag naar parttime werk.

De arbeidsvoorwaarden zijn over het algemeen gunstig. De salarisindicatie ligt tussen de 2.500 Euro en 6.000 Euro (bruto bij een 36- tot 40-urige werkweek). De salarisindicatie wordt echter zelden genoemd in de vacatureteksten.

3.2.6 Duiding en ontwikkeling van de vraag

Hoe organisaties omgaan met deze groep technisch dominante specialisten is, zo blijkt, op basis van interviews met organisaties, verschillend voor grote en kleinere organisa-

[80] NB: het gaat hier om voorbeelden. In het noemen van de specifieke bedrijven kan niet hun belang/belangrijkheid worden afgeleid.

ties. Daarnaast spelen de consultancybedrijven met betrekking tot deze groep een grote rol.

Een aantal grote bedrijven is groot genoeg om zelf technische dominante specialisten aan te nemen. Zij kunnen een interessant takenpakket bieden met voldoende uitdagend werk voor ethical hackers en pentesters. Voorbeelden van deze organisaties zijn de Rabobank, KPN, de Politie en Defensie. Deze grote organisaties hebben de afgelopen jaren Security Operations Centres (SOC's) opgezet, waarin professionals verantwoordelijk zijn voor monitoren, testen, analyseren en opvolgen van *cyber threats*. Bij Defensie (en deels bij de Politie) hebben deze professionals een afwijkend takenpakket omdat zij als enige in Nederland ook offensieve hack-activiteiten mogen ontplooien. In deze grote organisaties vindt veelal ook functiescheiding plaats, waarbij professionals in teams opereren (zie tekstbox).

Bij de Rabobank bestaat het SOC uit vier teams:
- *Monitoring: dit team bekijkt al het traffic en monitort de infrastructuur op vreemd gedrag. Het team kan tevens actie ondernemen of de informatie naar de verantwoordelijke doorsturen. Het kan gaan om DDoS aanvallen, Malware uitbraken, in- en extern misbruik van de infrastructuur. Het team bestaat uit elf medewerkers.*
- *Testers: alles wat gebouwd wordt, wordt eerst getest voordat het online gaat. Hierbij gaat het om alle tools, applicaties en websites, óók die van de lokale banken (deze worden getest als ze online zijn). In dit team zitten zeven testers en een coordinator.*
- *Encryptie: het verkeer tussen betalingssystemen is gecodificeerd. Dit team doet niets anders dan zorgen dat de versleuteling werkt. In dit team zitten zes medewerkers.*
- *Certificaten: dit team geeft certificaten en domeinnamen uit en doet aan brandprotection: hoe het merk zowel intern als extern wordt ge- of misbruikt. Dit team heeft vier medewerkers.*

Daarnaast zijn er twee productmanagers die de vertaalslag moeten maken van bedreigingen naar beveiliging.

Gegeven de verschillende functies binnen een SOC, bestaat een onderscheid tussen enerzijds de 'super-hacker' (dat is diegene die zonder protocol op hoog-technisch niveau lekken in ICT-systemen probeert te vinden) en anderzijds de professionals die meer gestandaardiseerd werk doen. Eenzelfde onderscheid doet zich voor in de cybercrime: enerzijds gerichte, creatieve en innovatieve hoog-technische aanvallen, anderzijds aanvallen die gebruik maken van het standaardrepertoire van tools en technieken.

Ondanks dat grote organisaties een aantrekkelijk takenpakket kunnen bieden voor de groep technisch dominante specialistische Cyber Security Professionals, ondervinden grote organisaties grote moeilijkheden om de vacatures te vervullen. Vooral als het gaat om hele specifieke expertise blijkt het lastig mensen te vinden (bijvoorbeeld expertise op SCADA, specifieke programmeertalen). Defensie heeft daarnaast moeite snel te handelen, doordat assessments en integriteitsonderzoeken lang duren. Voor overheidsdiensten is het vaak lastig om te gaan met hogere salariseisen doordat salarisschalen gekoppeld zijn aan opleidingsniveaus (specialistische hackers hebben in veel gevallen geen diploma op het niveau waarop zij werken en denken).

Het opzetten van SOCs en teams van CSP's vraagt vaak om een aanpassing van de organisatiecultuur. Het is een romantisch beeld te denken in termen van zitzakken, cola en pizzadozen, maar organisaties geven aan dat enige aanpassing, met name in hiërarchische verhoudingen en mate van autonomie, noodzakelijk is om hackers aan te trekken en te behouden voor de organisatie.

Kleinere organisaties huren deze technisch dominante cybersecurity specialisten veelal in om specifieke opdrachten uit te voeren. Zij hebben onvoldoende interessant en uitdagend werk voor deze professionals om hen zelf aan te stellen. Daarnaast willen bedrijven juist professionals die in meerdere organisaties hebben rondgekeken en daardoor goed op de hoogte zijn van veranderende dreigingen en oplossingsmogelijkheden. Daarom spelen bij deze functiegroep de dienstverlenende bedrijven een grote rol (zoals Fox-IT, Pinewood, Digital investigations, Deloitte, Sogeti etc.)[81]. Getalenteerde hackers en cybersecurityspecialisten weten wat zij waard zijn, zij opereren als zelfstandige en laten zich inhuren voor specifieke klussen. Essentieel is dat binnen de kleinere organisaties expertise aanwezig is om externe expertise in te huren. Hierbij gaat het om het erkennen van de noodzaak om externen in te huren, maar ook om het omschrijven van de taken die externen moeten uitvoeren. Uit interviews komt naar voren dat deze expertise vooral bij kleinere organisaties ontbreekt (men weet eigenlijk niet wat men moet vragen).

Wat betreft de ontwikkeling van de vraag in de toekomst, kwam tijdens de interviews naar voren dat steeds meer hacker-handwerk in geautomatiseerde tools opgenomen wordt. Dit betekent dat penetratietesten vaker gestandaardiseerd uitgevoerd kunnen worden. Echter, doordat de cybercrimineel ook niet stil zit, zullen er altijd nieuwe dreigingen naar voren komen die de hacker en tester zullen moeten opsporen en onschadelijk maken. Een nieuw terrein van onveiligheid zijn apps en telefoonapps. Deze zijn vaak slecht beveiligd en geven toestemming om privacygevoelige informatie te gebruiken. Als kleinere organisaties beter toegerust zijn op het omgaan met cybersecurity, zal ook bij hen het bewustzijn toenemen dat regelmatig externen ingehuurd moeten worden om testen uit te voeren. Bij grotere organisaties zal, doordat men het testen intern kan organiseren, de vraag naar externe hackers juist afnemen.

Daarom zal de vraag naar deze groep professionals waarschijnlijk, ondanks verdere automatisering en standaardisering van cybersecurity, zowel op korte, middellange, en lange termijn toenemen. Waarschijnlijk zullen grote organisaties en zakelijke dienstverlening het grootste aandeel van de werkgelegenheid vormen. Kleinere organisaties zullen vooral gebruik maken van inhuur van externen.

3.3 Arbeidsmarkt voor niet technisch dominante specialistische cybersecurityfuncties (functiegroep 2)

In de vacature-analyse zijn veel functies geïdentificeerd die als niet technisch dominant en specialistisch kunnen worden gekarakteriseerd. Hierbij gaat het om functies die zowel operationeel/tactisch als tactisch/strategisch van aard zijn. Binnen dit domein komen we de volgende functies/omschrijvingen tegen op de verschillende niveaus:

- *Operationeel-tactisch niveau* (security officer, informatie-analist, beveiligingsbeambte, specialist ICT, consultant, cybercrime-adviseur, consultant cybersecurity and data communication).
- *Tactisch-strategisch niveau* (hoofd informatievoorziening, accountmanager IT, coordinator informatiebeveiliging, manager analytics, manager new technology & security).
- *Zowel Operationeel-tactisch, als tactisch-strategisch niveau* (IT security specialist, business analist, security integration engineer).

Hierbij moet worden opgemerkt dat de titel 'IT-securityspecialist' overlap vertoont met de in functiegroep 1 ingedeelde ethical hacker. De IT-securityspecialist wordt vaak omschreven als een intermediair tussen de techniek en de organisatie, maar de functie is nog altijd wel behoorlijk technisch van aard. In deze functies gaat het om de interactie van mensen met ICT, waarbij de kern van de werkzaamheden strikt genomen buiten ICT

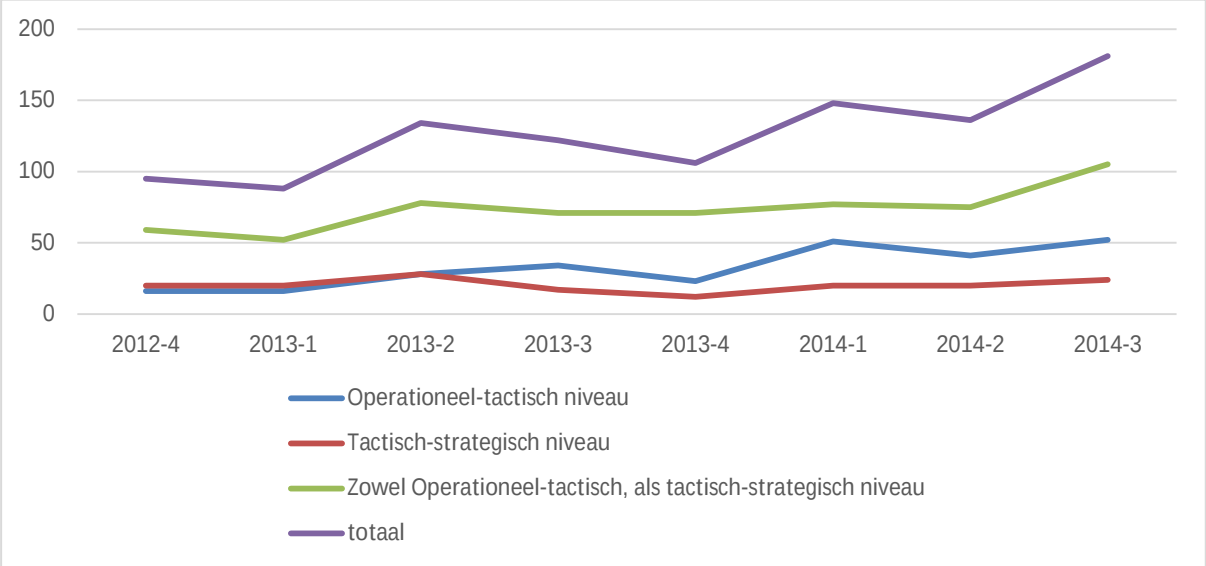
[81] NB: het gaat hier om voorbeelden. In het noemen van de specifieke bedrijven kan niet hun belang/belangrijkheid worden afgeleid.

en cybersecurity ligt, maar waarin ICT- en cybersystemen wel een grote rol spelen. In een onderzoek naar beroepsprofielen voor professionals in de informatiebeveiliging (Spruit en Van Noord, 2014)[82] wordt dit type werkveld aangeduid als 'ICT security'. Van den Berg (2014)[83] karakteriseert deze functie als socio-technisch.

3.3.1 Kwantitatief overzicht vacatures (aantallen en historisch overzicht)

Totaal waren er de afgelopen zeven kwartalen ongeveer 1.010 vacatures voor niet technisch dominante specialistische cybersecurityfuncties (functiegroep 2). Iets meer dan de helft (58%) kan als zowel operationeel-tactisch, als tactisch-strategisch gekenmerkt worden; ongeveer een kwart (26%) bestaat uit beroepen op operationeel-tactisch niveau en de rest (16%) bestaat uit functies op tactisch-strategisch niveau. Onderstaande figuur geeft de ontwikkeling van de vraag naar de verschillende functies binnen deze groep op de drie niveaus weer over zeven kwartalen (vierde kwartaal 2012 t/m derde kwartaal 2014).

Figuur 7: Vraag naar niet technisch dominante specialistische cybersecurityfuncties (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

Door de tijd heen is een toename van de vraag te zien. Werden er in het eerste kwartaal van 2013 nog 88 vacatures gepubliceerd, in de vergelijkbare periode in 2014 waren er 148 vacatures. Dit steeg nog verder tot 181 vacatures in het derde kwartaal van 2014. De stijging is vooral te zien bij de functietitels 'IT security specialist' (ongeveer verdrievoudigd tussen het eerste kwartaal 2013 en het derde kwartaal 2014 tot 98 vacatures) en 'security officer' (verviervoudigd, gestegen tot 40 vacatures in derde kwartaal 2014). Echter, opgemerkt moet worden dat het aantal gepubliceerde vacatures waarschijnlijk een onderschatting is van de totale vraag. Hierbij speelt een rol dat organisaties niet graag vacatures op deze functies publiekelijk uitzetten aangezien de vacature een zwakte van het bedrijf aangeeft ('security is niet op orde'). Daarom wordt ook via netwerken en headhunters geworven.

[82] Spruit, M. en F. van Noord (2014). Beroepsprofielen Informatiebeveiliging. In opdracht van PvIB en QIS.
[83] Van den Berg, Jan, Van Zoggel, Jacqueline, Snels, Mireille, Van Leeuwen, Mark, Boeke, Sergei, Van de Koppen, Leo, Van der Lubbe, Jan, Van den Berg, Bibi, De Bos, Tony, (2014), On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security EducationBerg, J. van den (juli 2014). PPT-presentatie 'Cyber Security Academy (CSA) The Hague: https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf

3.3.2 Functiebeschrijvingen

Als we naar de functieomschrijvingen kijken, komen we de volgende kerntaken tegen:

- *Communicatie en advies*: in veel functies dient de professional in staat te zijn helder te kunnen rapporteren over ICT en technische vraagstukken. Daarnaast hebben deze CSP's veelal een adviserende rol, zowel binnen hun eigen organisatie (opstellen securityjaarplannen), maar ook richting klanten/stakeholders. Binnen de organisatie hebben CSP's vaak een voorlichtende functie. Vaak wordt benadrukt dat de CSP zowel gevraagd als ongevraagd advies dient te geven.
- *Controleren*: vaak is de CSP verantwoordelijk voor het waarborgen van de informatiebeveiliging. Hierbij spelen (interne) audits een grote rol. Ook ligt hierin veelal een directe link met business continuity.
- *Samenwerken*: de functieomschrijvingen noemen vaak het opereren in teamverband, zowel binnen een organisatie, als tussen organisaties in netwerken.
- *Integriteit*: Ook integriteit en de voorbeeldfunctie van de security officer worden in vacatureteksten genoemd. Dit geldt vooral (maar zeker niet uitsluitend) voor overheidsvacatures. *Uitvoeren technische tests*: in een aantal gevallen wordt van de CSP verwacht dat hij/zij ook zelfstandig veiligheidstesten kan uitvoeren. Grondige ICT-kennis is daarom vaak een vereiste.

Daarnaast is er een aantal vacatures g*ericht op sales en marktver*groting (bijvoorbeeld in de functie 'accountmanager IT security').

In de tekst box hieronder staan een aantal exemplarische functieomschrijvingen voor de niet technische dominante specialistische cybersecurity professionals (functiegroep 2).

Als Security Specialist ben je betrokken bij diverse securityaspecten als intrusion prevention, intrusion detection en securitytesting. Een Security Specialist houdt zich verder bezig met samenwerking met de overheid en andere grote corporaties, het in control zijn met diverse vormen van cybercrime en het voorkomen van cyberaanvallen.

Als informatieanalist houdt jij je bezig met het uitwerken van vraagstukken op ICT-gebied tot zodanig concrete en haalbare voorstellen dat de opdrachtgever kan beslissen over haalbare inzet van ICT-systemen. Je brengt advies uit met betrekking tot de oplossingsrichting van aanvragen. Je werkt de inzet van ICT-systemen uit tot een volledig advies inclusief procesbeschrijving, informatiemodel en implementatiestadia. Vervolgens zet je het advies om in een ontwerp inclusief functionele specificaties en technische componenten die binnen Algemene Dienst ICT beschikbaar zijn dan wel beschikbaar te maken zijn.

Als Security Officer bij een financiële dienstverlener zorg je binnen een divisie voor het waarborgen van de informatiebeveiliging, zowel gericht op de bescherming van informatie als de continuïteit van de commerciële processen en informatievoorziening. Je bent volledig thuis in de security van de moderne E-business. Je weet bij het sluiten van contracten de securityaspecten te waarborgen. New business via het inzetten van mobile apps is je niet onbekend en je volgt op de voet de securityontwikkelingen. Je hebt kennis van penetratietesten op de E-business-omgeving en weet op basis van de testrapporten verbeteringen te realiseren.

3.3.3 Functie-eisen: opleidingsniveau en competenties

Wat betreft het gevraagde werk- en denkniveau blijkt dat in 25% van de vacatures een WO-niveau wordt gevraagd, 41% geeft een HBO-/WO-niveau aan, 29% vraagt een HBO-werk- en denkniveau, 4% vraagt om een MBO-/HBO-niveau en 1% vraagt om MBO-niveau. Ten slotte werd er voor vier vacatures een post-WO werk- en denkniveau gevraagd.

Veel voorkomende eisen in vacatureteksten zijn:

- *Technische ICT-kennis*, zoals kennis van internet en computernetwerken. Veel vacatures specificeren de vereiste kennis van programmatuur, talen, standaarden en pakketten.
- *Brede kennis van dreigingen*: kennis van dreigingen en risico's met betrekking tot computernetwerken en organisatieaspecten binnen het werkveld van de werkgever en kennis van de maatregelen die je daartegen kunt nemen wordt als zeer belangrijk ervaren.
- *Kennis van of ervaring met het werkveld van de werkgever*: hierbij gaat het om het kunnen plaatsen van de cybersecurity in de organisatorische context: wat is belangrijk en wat is het doel van cybersecurity in de organisatie.
- *Kennis van wet- en regelgeving* op het gebied van IT-security, privacy en het werkveld van de werkgever.
- *Communicatieve vaardigheden*: de specialist wordt verwacht gestructureerd te kunnen schrijven en in gesprekken helder een boodschap over te brengen, zowel in het Nederlands als Engels.
- *Autonomie*: dit betekent zowel het zelfstandig oplossen van problemen, als het gevraagd en ongevraagd advies uitbrengen.
- *Andere vereiste attitudes* zijn initiatiefrijk, samenwerken, resultaatgericht, onderzoeksminded, omgevingssensitiviteit, begrip van ethisch handelen.
- *Ervaring*: veel vacatures vragen om ervaring. Vaak wordt vijf jaar ervaring gevraagd, of in ieder geval drie jaar.
- *Certificaten en omgang met ISO/NEN normen* worden ofwel vereist, ofwel als een pré beschouwd.

Als relevante HBO-/WO-opleiding wordt informatica of bedrijfskundige informatica genoemd; vaak wordt echter niet aangegeven wat een relevante opleiding is.

Bij de meer tactisch-strategische functies komen algemene leidinggevende eigenschappen naar voren, zoals het kunnen leidinggeven aan medewerkers in project- of teamverband, het motiveren van medewerkers of het hebben van een goed gevoel voor de organisatorische, functionele, bestuurlijke en politieke verhoudingen binnen de organisatie.

Uit de functie-eisen blijkt ook dat de niet technisch dominante cybersecurityspecialist een dubbelrol heeft: hij/zij is een intermediair tussen de organisatie in de brede zin en de ICT-afdeling. Dit komt bijvoorbeeld tot uiting de volgende omschrijving van functie-eisen.

Security Officer Commerce […]

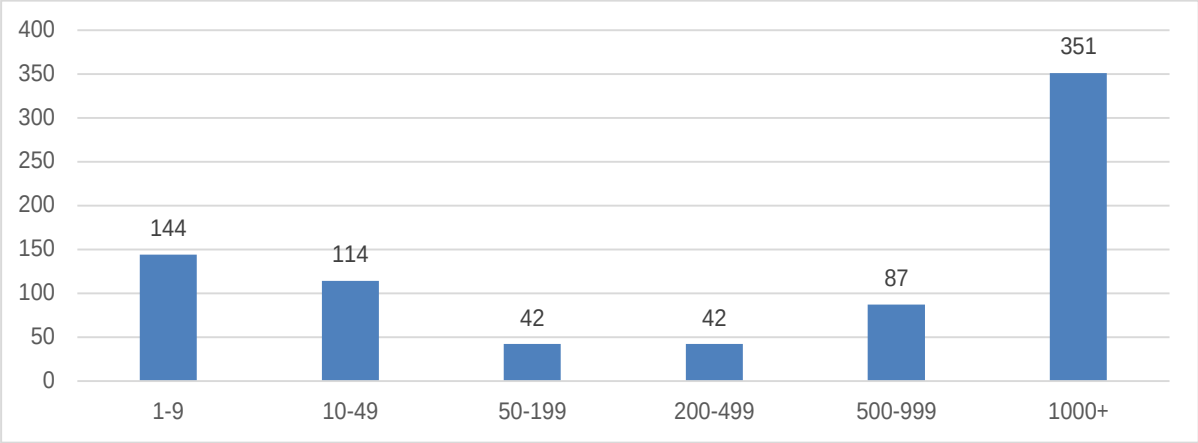
- *Naast procedurele kennis van informatiebeveiliging heb je ook technische IT-basiskennis, zodat je een volwaardig gesprekspartner bent van IT-professionals.*
- *Je bent een gedreven pragmaticus en weet met een open stijl en flexibele houding jezelf op alle niveaus (directie, management, uitvoerend) te presenteren en stakeholders te overtuigen en beïnvloeden.*
- *Multidisciplinair kunnen denken en communiceren.*
- *Gestructureerd en planmatig kunnen denken en werken.*
- *Je bent communicatief sterk en benaderbaar en creëert een basis van vertrouwen Je hebt oog voor de belevingswereld van de organisatie, daarbij zoek je de optimale afstemming tussen securitybelangen en andere bedrijfs- c.q. commerciële belangen. Indien nodig ga de confrontatie niet uit de weg en blijf je onder druk effectief functioneren […].*

Voor deze dubbelrol, het zowel kennen van de organisatie als technisch onderlegd zijn, is ervaring vereist.

3.3.4 Profiel werkgevers

De niet technisch dominante specialistische Cyber Security Professionals worden voornamelijk gevraagd binnen de ICT (22%), zakelijke dienstverlening (12%), financieel / verzekeringen (12%), overheid (5%) en handel (6%). Voorbeelden van organisaties die veel vacatures hebben gepubliceerd zijn de Rabobank, Achmea, ASR, Belastingdienst, Ministeries, ASML, Verizon[84]. Ten aanzien van deze functie moet worden opgemerkt dat veel bedrijven maar een beperkt aantal van deze professionals nodig hebben om de schakel te kunnen vormen tussen techniek en organisatie. Deze professionals kunnen nogal eens opereren als 'eenlingen' binnen de organisatie. In onderstaande figuur is de verdeling van vacatures naar organisatiegrootte weergegeven.

Figuur 8: Totaal aantal vacatures voor niet technisch dominante specialistische cybersecurityfuncties naar organisatiegrootte (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

Uit bovenstaande figuur blijkt dat vooral de grote organisaties vacatures voor niet technisch dominante specialistische cybersecurityfuncties te vervullen hebben. Zij zijn verantwoordelijk voor 35% van de totale vraag. Echter binnen de groep 1000+ bedrijven is de dynamiek anders dan bij andere functiegroepen: het totaal aantal grote bedrijven is groter en het aantal vacatures per bedrijf is lager: het vacatureaanbod wordt minder gedomineerd door de dienstverlenende bedrijven.

3.3.5 Arbeidsvoorwaarden

Wat betreft het voorziene dienstverband blijkt uit de vacature-analyse dat meer dan 80% van de vacatures een fulltime dienstverband (>32 uur) in het vooruitzicht stelt. Bij 10% is zowel fulltime als parttime een optie. In 10% van de vacatures gaat het om een dienstverband van minder dan 32 uur. In vergelijking met de arbeidsmarkt in het algemeen is er weinig vraag naar parttime werk.

De arbeidsvoorwaarden zijn over het algemeen gunstig. De salarisindicatie ligt tussen de 2.300 Euro en 5.600 Euro (bruto, op basis van een aanstelling van 36 tot 40 uur per week), waarbij de private sector meer lijkt te betalen dan de publieke sector. Daarnaast worden vaak aanvullende opleidingen en cursussen aangeboden.

3.3.6 Duiding en ontwikkeling van de vraag

Uit de interviews blijkt dat dit type functie (niet technisch dominante specialistische cybersecurityfuncties) aanwezig is in veel (grote) organisaties. Dit type professional fungeert vaak als intermediair tussen de organisatie en de ICT-afdeling. Een goede, grondige kennis van het werkveld van de werkgever is daarbij onontbeerlijk. Hierdoor worden

[84] NB: het gaat hier om voorbeelden. In het noemen van de specifieke bedrijven kan niet hun belang/belangrijkheid worden afgeleid.

security officers soms intern geworven (uit systeembeheerders met interesse voor security), of wordt de recruitment gevolgd door een grondige introductieperiode (doorlopen werkproces van de organisatie). Voor veel organisaties is het aanstellen van de security officer één van de eerste stappen om daadwerkelijk systematisch aan security te werken. Problematisch hierbij is dat de organisaties eigenlijk niet de kennis en ervaring hebben om te weten wat zij precies moeten verwachten van een security officer. Uit interviews blijkt dat hierdoor het opstellen van het functieprofiel vaak naar de ICT-kant uitslaat.

Vaak is deze niet technisch dominante specialistische cybersecurity professional organisatorisch ingedeeld in de ICT-afdeling. In veel gevallen heeft deze professional wel een onafhankelijke rol en rapporteert hij/zij direct aan de directie. Bij één organisatie was de functie ingedeeld bij de fysieke beveiligingsafdeling, omdat fysieke beveiliging gebruik maakt van verschillende ICT-middelen (biometrische toegangsmethoden, cameratoezicht, elektronische toegangspoorten en deuren etc.). In het algemeen heeft de niet technisch dominante cybersecurity specialist de rol van 'luis in de pels', een onafhankelijke medewerker die gevraagd en ongevraagd advies mag geven over beveiliging. Daarnaast heeft deze professional vaak een communicatieve functie naar de andere medewerkers, om hen bewust te maken van gevaren in omgaan met ICT-systemen.

Het aanstellen van een medewerker in deze functie is in veel organisaties de eerste stap op het gebied van cybersecurity. Hierdoor zijn deze professionals vaak eenlingen in de organisatie en missen zij sparringpartners binnen de organisatie. Om veranderingen in gang te zetten binnen de organisaties, moeten zij over goede communicatieve vaardigheden beschikken. Door het gebrek aan interne sparringpartners zien we bij een aantal typen organisaties, zoals gemeenten, intra-organisatie-overlegstructuren ontstaan waarin cybersecurity-issues worden besproken.

Ondanks dat de nadruk vaak op ICT ligt, geven professionals zelf aan dat het beter is om over 'information-security' te spreken dan over 'IT-security'. Dit omdat het uiteindelijk gaat om informatie, niet om de IT erachter. De kern is het veiligstellen van de beschikbaarheid van informatie, de integriteit van informatie en de veiligheid van informatie. Hierbij overstijgt de functie de klassieke netwerkbeheerder. De nadruk op de techniek is ambigue. Aan de ene kant wordt door professionals benadrukt dat wanneer je IT-security vanuit het management benadert, je dan te weinig kennis van techniek hebt om goede afwegingen te maken en de juiste vragen te stellen aan ICT'ers en ontwikkelaars. Daarbij is het lastig deze ICT-kennis op te doen als je geen ICT-achtergrond hebt. Aan de andere kant is de veiligheidsoplossing nooit direct een ICT-oplossing. De techniek kan een gevolg zijn van een oplossing. Minder goed ingevoerde information security officers denken vaak in termen van oplossingen door techniek, maar een goede CSP ziet de techniek als een gevolg van de gekozen oplossing.[85]

Gegeven de sterke link met het werkveld, is er nog altijd een grote rol weggelegd voor zakelijke dienstverlening. Consultancy- en detacheringsbedrijven worden ingehuurd om organisaties in te richten om hun informatiebeveiliging op te zetten. De adviseurs zijn hierin niet de hackers (zie functiegroep 1: technische dominante specialisten), maar eerder organisatiekundigen, bedrijfskundigen met affiniteit met techniek. Vaak bieden certificaten de garantie dat zij zowel de cybersecuritykennis als organisatorische kennis hebben om organisaties te adviseren (CISSP, CISA, CISM etc.).

De nadruk op privacywetgeving[86] en het hanteren van ISO-normen (2700x) leidt tot het aanstellen van meer personen in deze functie. Veel publieke organisaties, zoals gemeen-

[85] Typerend is het citaat van Bruce Schneider: "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." Read more at http://www.brainyquote.com/quotes/authors/b/bruce_schneier.html#Gj4XtXSoaWM2u7xR.99

[86] Organisaties zijn zich aan het voorbereiden op het omgang met de nieuwe Europese Privacy richtlijn. Deze richtlijn zal aanzienlijke consequenties hebben voor hoe bedrijven omgaan met privacy. Het ziet er naar uit dat het niet opvolgen van de nieuwe richtlijn resulteert in aanzienlijke boetes. Investeren in security wordt daarmee in plaats van een kostenpost een besparingsmaatregel.

ten, worstelen met de beveiliging van hun ICT-systemen. Zij hanteren veel verschillende systemen waar privacygevoelige informatie ligt opgeslagen, maar missen vaak de expertise (en middelen) om dedicated Cyber Security Professionals met een technisch profiel aan te stellen. De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), gebaseerd op ISO-normen aangevuld met aanvullende eisen, biedt een goed houvast voor gemeenten om hun beveiliging vorm te geven. Deze baseline dient echter in de toekomst verder ontwikkeld te worden, om echt informatiebeveiligingsbewustzijn binnen publieke organisaties te versterken.

De verwachting is dat er door toename van incidenten, het toenemend bewustzijn van het belang van informatiebeveiliging, hogere regeldruk vanuit overheid, verzekeringen en leveringscontracten[87], ook bij kleinere organisaties meer nadruk komt om het vormgeven van cybersecurity. Hierdoor zullen meer security officers worden aangesteld. Zoals aangegeven gaat het hierbij niet om technische dominante professionals, maar professionals die de bedrijfsrisico's kunnen interpreteren in termen van ICT-systemen. De verwachting is dat op de korte en middellange termijn de vraag naar deze professionals stijgt, echter dat in veel gevallen deze functie intern wordt ingevuld door ofwel iemand binnen de ICT-afdeling, ofwel door iemand binnen het management verantwoordelijk te stellen voor cybersecurity en informatiebeveiliging. De vraag naar deze professionals op de lange termijn is onduidelijk. Mogelijk zal de vraag naar deze functie afnemen als iedere organisatie het belang van cybersecurity heeft onderkend en een security officer heeft aangesteld.

3.4 Arbeidsmarkt technisch dominante functies waarbij cybersecurity een onderdeel is (functiegroep 3)

Naast een vraag naar specialistische functies, is er een aanzienlijke behoefte aan professionals voor technisch dominante functies waarin cybersecurity een onderdeel van het werk is. Een criterium is of cybersecurity-certificaten ofwel vereist zijn, ofwel een pré vormen. De aanname is dat als deze certificaten gevraagd worden, ten minste bij een deel van de werkzaamheden veiligheidsaspecten aan de orde komen. Ten aanzien van deze technische dominante functies waarin beveiliging enkel een deelaspect is, kan het gaan om functies op operationeel-tactisch en tactisch-strategisch niveau. In de vacatureanalyse komen we, ten aanzien van deze niveaus, de volgende omschrijvingen van beroepen tegen:

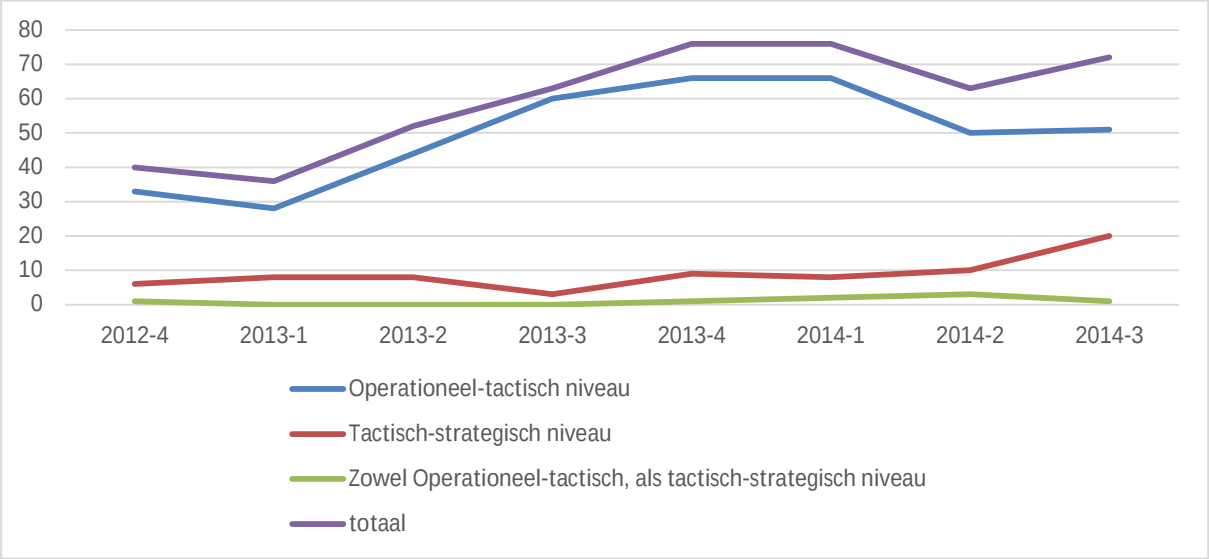
- *Operationeel-tactisch niveau*: ICT-consultant, systeemarchitect, infrastructuurspecialist, netwerkspecialist algemeen, software engineer, routing ingenieur, systeembeheerder, systems engineer, IT-specialist, applicatiebeheerder, functioneel applicatiebeheerder.
- *Tactisch-strategisch niveau:* manager ICT, keurder interne controleafdeling, projectleider automatisering, projectleider netwerk- en systeembeheer.
- *Zowel operationeel-tactisch, als tactisch-strategisch niveau:* BI-specialist datawarehouse.

[87] De rol van het verzekeren van cyberrisico's is een opkomend fenomeen, waarbij het inschatten van risico's tot dezelfde problemen leidt als het inschatten van de kosten van cybercrime. Waar een aantal risico's afgedekt wordt door traditionele verzekeringen, zijn er ook cyberrisico's die buiten de traditionele dekking vallen (Verbond van Verzekeraars (2013). Position paper: Virtuele risico's, echte schade; Over het verzekeren van cyberrisico's). Het betreft hier schade door: 1) een moedwillige aanval van buitenaf, bijvoorbeeld een virus, DDoS-aanval of een hack; 2) een menselijke fout, al dan niet opzettelijk, waaronder verlies of diefstal van (een onderdeel van) een computersysteem of data van de verzekerde die persoonsgegevens bevatten; 3) technisch falen van eigen of externe IT-systemen, servers, hard- en software. Bovengenoemde incidenten leiden tot een verlies van of beschadiging aan data, (on)toegankelijkheid van systemen, aansprakelijkheid, bedrijfsschade, afpersing en boetes. Dat zijn allemaal zaken die geld kosten. Verzekeraars zijn momenteel bezig deze verzekeringen (verder) te ontwikkelen. De verwachting is dat hierbij ook kwesties aan de orde komen over garanties met betrekking tot beveiliging van (bedrijfs)systemen (bijvoorbeeld certificaten en kwalificaties). Hieraan gerelateerd zijn ontwikkelingen in aanbestedingseisen (door overheid én bedrijfsleven). Doordat organisaties zich willen beschermen tegen cyberrisico's worden ook eisen gesteld aan toeleveranciers. Hierdoor wordt cybersecurity belangrijker voor MKB-ondernemingen (zie bijvoorbeeld: http://www.beschermjebedrijf.nl/).

3.4.1 Kwantitatief overzicht vacatures (aantallen en historisch overzicht)

In totaal gaat het in deze functiegroep om 478 vacatures over de afgelopen zeven kwartalen. Het operationeel-tactische niveau is sterk vertegenwoordigd (83%), slechts 15% van de vacatures vraagt om tactisch-strategisch niveau van opereren. Ten slotte is nog geen 2% als beide geclassificeerd. Onderstaande figuur geeft de ontwikkeling van het aantal vacatures over de afgelopen zeven kwartalen weer.

Figuur 9: Vraag naar technisch dominante functies waarbij cybersecurity een onderdeel is (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

Uit bovenstaande figuur blijkt dat er in het laatste kwartaal van 2013 en eerste kwartaal van 2014 een grote vraag was. Daarna, in het tweede kwartaal van 2014 (vooral als het gaat om de operationeel-tactische functies) komt minder vraag tot uiting in Jobfeed. In het derde kwartaal van 2014 nam de vraag weer iets toe. De vraag naar functies op tactisch-strategisch niveau neemt geleidelijk toe van 6 vacatures in het laatste kwartaal van 2012 tot 20 vacatures in het derde kwartaal van 2014. Ook ten aanzien van deze functiegroep geldt dat het aantal genoemde vacatures een onderschatting van de totale vraag kan betreffen. Veel afgestudeerden van HBO en WO stromen direct in vanuit opleiding en/of stage zonder dat er een vacature gepubliceerd wordt. Dit is karakteristiek voor de gehele ICT sector.

3.4.2 Functiebeschrijvingen

In de functieomschrijvingen van deze groep vacatures komen we net andere kerntaken tegen dan in de eerder besproken functiegroepen. In deze groep van technisch dominante functies waarbij cybersecurity een onderdeel is, ligt het accent op:

- *Inrichten en beheren van systemen*: hierbij hoort tevens het beschikbaar en veilig houden van de systemen. De CSP dient de balans in de gaten te houden tussen beveiliging en gebruiksgemak. Ook wordt het omgaan met migraties van systemen als een aspect genoemd.
- *Secure houden van ICT systemen*: hierbij gaat het vooral om network security, zoals firewalling, VPN en encryptie. Ook het omgaan met privacy en autorisatierollen wordt hierin genoemd.
- *Beleidsontwikkeling op het gebied van ICT*: met name de meer tactisch-strategische functies richten zich op bredere beleidsontwikkeling t.a.v. de ICT, waarin beveiliging een onderdeel vormt.

Onderstaande functieomschrijving illustreert de mate waarin beveiliging binnen een bredere functie wordt ingebed.

Als Senior medewerker Informatisering & Automatisering (I&A) houd je de interne (beleids)ontwikkelingen in de gaten en vertaal je deze naar de wereld van informatisering en automatisering. Daarnaast ben je het inhoudelijk aanspreekpunt en coach voor de medewerkers I&A. Je verdeelt de werkzaamheden en stelt daarbij de prioriteiten voor de uit te voeren I&A-activiteiten. Hierbij kun je denken aan zaken als informatiebeveiliging, applicatiebeheer, implementatie van nieuwe programmatuur, incidentenbeheer, informatieanalyse en ontwerpen en ontwikkelen van toepassingen die niet op de markt zijn.

3.4.3 Functie-eisen: opleidingsniveau en competenties

Bij technisch dominante functies waarbij cybersecurity een onderdeel van het werk is, is het gevraagde werk- en denkniveau is vergelijkbaar met het gevraagde niveau voor de technisch dominante specialistische functies (functiegroep 1). In 19% van de vacatureteksten wordt een WO-achtergrond verlangd. 42% vraagt om HBO-/WO-niveau, 34% om HBO-niveau en 5% vraagt om een MBO-/HBO-niveau. Ook hier geldt dat op tactisch-strategisch niveau het werk- en denkniveau hoger ligt. De vergelijkbaarheid met de specialistische functies wijst erop dat de functies vergelijkbaar zijn op hoofdlijnen. De verschillen kunnen gevonden worden in de precieze functie- en competentie-eisen.

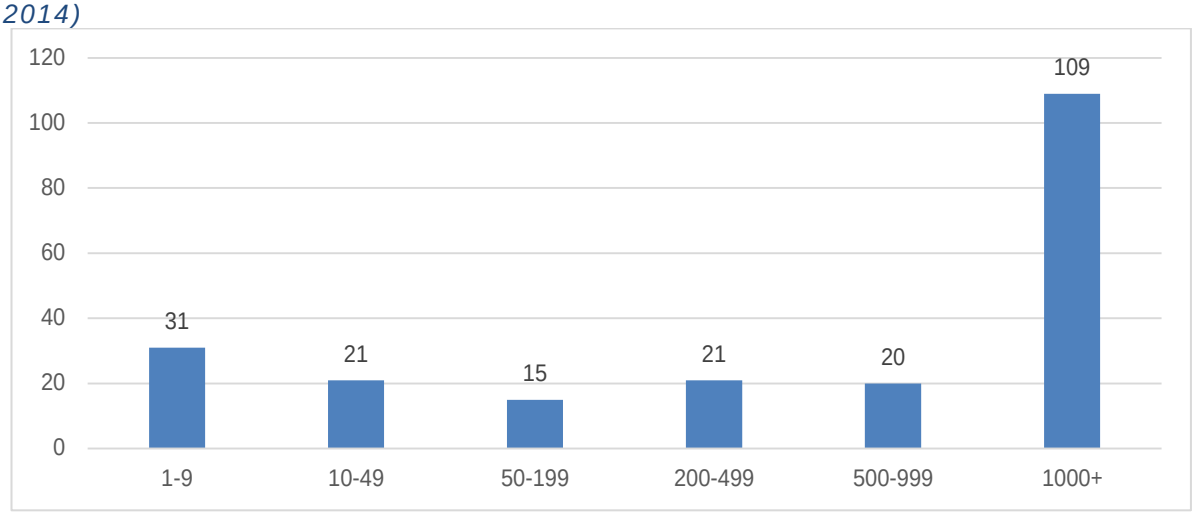
In vergelijking met de cybersecurityspecialisten, ligt de nadruk in de functie-eisen bij deze functiegroep meer op de ICT-kennis en ervaring met complexe netwerksystemen. Een minder grote nadruk ligt op communicatieve vaardigheden zoals gestructureerd kunnen schrijven en helder rapporteren. Het beveiligingsaspect komt vaak tot uiting in het eisen van een certificaat, ook wordt de beveiliging altijd in relatie gezien tot het netwerk en de ICT-omgeving. In de cybersecurityspecialist kwam vaker het organisatieperspectief naar voren. In het algemeen wordt ook minder gevraagd naar kennis van het werkveld van de werkgever (in een enkel geval wordt 'affiniteit met' genoemd).

3.4.4 Profiel werkgevers

De ICT-branche is ook hier de grootste werkgever (27%). Opvallend is dat de overheid ook een aanzienlijke speler is (6%). Voorbeelden van organisaties waar vacatures zijn verschenen zijn IBM, NS, Triodos Bank, NUON en grote software ontwikkelaars (zoals ATOS) en consultancybedrijven (bijvoorbeeld Capgemini) [88]. De afhankelijkheid van organisaties van ICT in hun bedrijfsvoering neemt toe. Hierdoor hebben niet alleen traditionele softwareontwikkelaars ICT'ers nodig, maar ook organisaties uit andere sectoren.[89] In onderstaande figuur is de verdeling van vacatures naar organisatiegrootte weergegeven.

[88] NB: het gaat hier om voorbeelden. In het noemen van de specifieke bedrijven kan niet hun belang/belangrijkheid worden afgeleid.
[89] Een illustratie hiervoor is de ledenlijst van Nederland ICT. De 582 leden zijn afkomstig uit verschillende sectoren waarin ICT een rol speelt: http://www.nederlandict.nl/?id=9152

Figuur 10: Totaal aantal vacatures voor technisch dominante functies waarbij cybersecurity een onderdeel is, naar organisatiegrootte (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

Uit bovenstaande figuur komt naar voren dat meer dan 33% van de vacatures voor rekening komt van organisaties met meer dan 1.000 medewerkers. Echter ook het kleinbedrijf (tot 50 medewerkers) is verantwoordelijk voor een groot deel van de vacatures (in totaal 32%).

3.4.5 Arbeidsvoorwaarden

Kijkend naar het dienstverband, dan geldt precies hetzelfde als bij de technisch dominante specialistische CSP functies, namelijk dat het in 81% van de vacatures gaat om een fulltime functie. De salarisindicatie ligt iets hoger dan bij de cybersecurityspecialisten (ongeveer tussen 3.500 tot 5.500 Euro bruto, op basis van een aanstelling van 36 tot 40 uur per week).

3.4.6 Duiding en ontwikkeling van de vraag

In de interviews met werkgevers en CSP's kwam vaak aan de orde dat ICT, ondanks het uitdijende vakgebied, nog een relatief jong vakgebied is, waarin security nog weinig aandacht heeft gekregen. ICT staat nog altijd in de kinderschoenen. Het is sterk aan het ontwikkelen zonder dat er heldere protocollen en spelregels zijn. Daarnaast kampt de ICT met 'legacy-problems'. Software is vaak niet geprogrammeerd met beveiliging in het achterhoofd, er bestaat veel programmatuur dat slordig is opgesteld, gebruik maakt van ad hoc oplossingen om problemen te voorkomen en systemen zijn zo aan elkaar geknoopt dat beveiligingsfouten gemakkelijk optreden. De zwakheid van veel huidige systemen zit in het feit dat ieder system een historisch system is, gebaseerd op integratie van oude systemen, ontwikkeld met andere veiligheidseisen in het achterhoofd. Tenslotte zijn ICT'ers opgeleid om te denken in termen van functionaliteit en gebruiksgemak, niet in termen van veiligheid.

In de vacature-analyse komt naar voren dat bedrijven vragen om systeembeheerders met een affiniteit met beveiliging. Tijdens de interviews wordt gewezen op de gevaren van het verantwoordelijk maken van traditionele systeembeheerders voor de IT-beveiliging. Zij kijken namelijk niet naar veiligheid zoals een hacker dat zou doen. Hun eerste zorg is de functionaliteit, of iets werkt, en niet de integriteit of waar het kapot kan. Cybersecurity vraagt een andere mind-set van ICT'ers in het algemeen: de vraag die aan deze professionals gesteld zou moeten worden, is waar en hoe zij zelf zouden inbreken als zij hacker zouden zijn.

Veel bedrijven zien ICT nog altijd als een ondersteunende afdeling; ondersteunend aan het primaire bedrijfsproces (net als HR en financiën). Dit is in veel gevallen echter onterecht: ICT is vaak het fundament van het bedrijf, óók wanneer ICT niet de core business van het bedrijf vormt.

De verwachting is dat veiligheidsaspecten binnen ICT een grotere rol zullen gaan spelen en dat software meer en meer de balans zoekt tussen functionaliteit en veiligheid (en integriteit van informatie). Echter, in dit domein is nog een grote slag te maken. Ook opdrachtgevers van softwareontwikkelaars (bedrijven, overheid) zullen in de toekomst bewuster omgaan met veiligheidsaspecten van hun ICT-oplossingen. Deze nadruk op veiligheidsaspecten zal op korte, middellange, en lange termijn zijn weerslag hebben op de vraag naar professionals die weet hebben van cybersecurity. De verwachting is dat de groei over vijf jaar wellicht iets sterker zal zijn. Er zijn dan meer organisaties die cybersecurity en informatiebeveiliging goed binnen hun organisatie hebben ingebed. Daarna zal deze functie meer en meer als algemene taak in het werken met software worden opgenomen.

3.5 Arbeidsmarkt niet technisch dominante functies waarbij cybersecurity een onderdeel is (functiegroep 4)

Net als bij functiegroep 3 kan bij deze functiegroep (functiegroep 4) een certificaat gevraagd worden in de vacaturetekst. Het gaat in deze groep echter vaak niet om het tonen van technische ICT-kennis (programmeren, architectuur, systeembeheer), maar eerder om het valideren van systemen en organisaties, het leiden van specifieke projecten, of het in algemene termen beoordelen van cybersecurity op organisatieniveau.

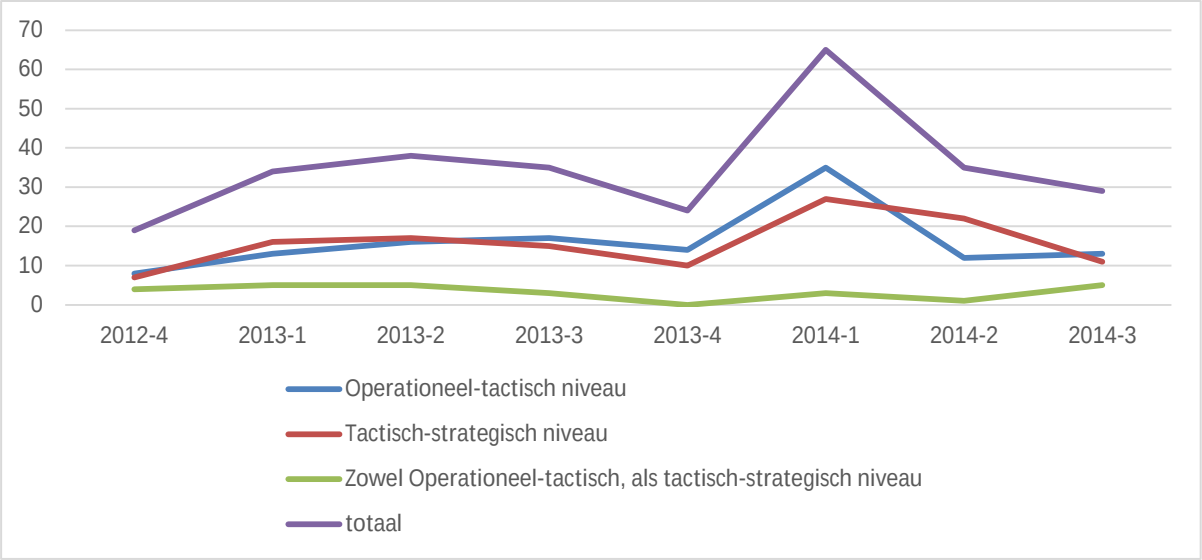
Onderscheiden naar de functieniveaus, komen we in deze functiegroep de volgende beroepen tegen:

- *Operationeel-tactisch niveau*: IT auditor, auditor, risk manager, internal auditor, sales engineer.
- *Tactisch-strategisch niveau:* bedrijfsadviseur, projectleider informatievoorziening, hoofd audit en control, projectleider (securityprojecten).
- *Zowel operationeel-tactisch, als tactisch-strategisch niveau:* management consultant, adviseur.

3.5.1 Kwantitatief overzicht vacatures (aantallen en historisch overzicht)

In totaal zijn in de laatste zeven kwartalen voor deze functiegroep (niet technisch dominante functies waarbij cybersecurity een onderdeel is) 280 vacatures gevonden. De helft (50%) van deze vacatures is als operationeel-tactische geclassificeerd en iets minder dan de helft (42%) als tactisch-strategisch. Minder dan 1% is als beide geclassificeerd. Onderstaande figuur geeft de ontwikkeling van het aantal vacatures over de afgelopen zeven kwartalen weer.

Figuur 11: Vraag naar niet technisch dominante functies waarbij cybersecurity een onderdeel is (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

De vraag naar deze groep CSP's laat een piek zien in het eerste kwartaal van 2014. Het aantal vacatures steeg van 24 in het laatste kwartaal van 2013 tot 65 in het daaropvolgende kwartaal. Hierna daalde de vraag twee kwartalen op rij naar 29 vacatures in het derde kwartaal van 2014. Bij deze functie kan het zijn dat de vraag niet geheel tot uiting komt in vacatures en functieomschrijvingen, maar in het aanpassen van het takenpakket van bestaande functies.

3.5.2 Functiebeschrijvingen

In de functieomschrijvingen van deze groep vacatures komen verschillende aspecten naar voren. Zo zijn er omschrijvingen die gericht zijn op het uitvoeren van audits waarin risicoanalyses worden uitgevoerd, waarbij moet worden gekeken naar de omgang met fraude en forensisch onderzoek en algemene netwerkbeveiliging. Deze organisatie-interne auditors rapporteren veelal direct aan de Directie of Raad van Bestuur. Ten slotte is er een groot aantal vacatures zoals beleidsadviseur, strategisch informatiemanager, manager directiestaf, bedrijfsadviseur waarin cybersecurity een deelaspect is van het totale takenpakket.

Als beleidsadviseur ga je zelfstandig bezig met visievorming, agendering, bewustwording en het oplossen van een aantal vraagstukken op het gebied van de informatiebeveiliging. Tevens zorg je er als beleidsadviseur voor dat er oplossingen worden gerealiseerd en geborgd.

De manager Directiestaf zorgt voor een goede verbinding tussen de Directiestaf en de Business en tussen Directieraad en de Raad van Commissarissen. In deze functie rapporteer je hiërarchisch aan de Directeur Concernzaken en functioneel aan de Statutaire directie. Je bent verantwoordelijk voor het opstellen, bijhouden en bewaken van het compliance kader en adviseert hierover in de bestuurlijke geledingen binnen de organisatie. Je bent verantwoordelijk voor het governance gedeelte van het informatiebeveiligingsbeleid. Daarnaast draag je zorg voor de publicatie en actualisatie van governance documenten op de website en screen je (corporate) communicatie vanuit een compliance invalshoek.

Als Juridisch beleidsmedewerker werk je mee aan nieuwe wet- en regelgeving voor informatiebeveiliging van digitale diensten bij de overheid. Zo werk je samen met de

collega's in het team Veiligheid van de afdeling Informatie aan het veilig houden van de overheidsdienstverlening. Als juridisch beleidsmedewerker ontwikkel je samen met de andere spelers in de openbare sector nieuw beleid. Als jurist maak je de afweging welk instrument het beste ingezet kan worden om de veiligheid te garanderen. Jouw taken zijn het onderkennen van juridisch relevante aspecten bij het onderwerp informatiebeveiliging, verbanden en achtergronden zien en conclusies trekken. Ook doe je onderzoek naar bestaande (sectorale) wetgeving op het aspect van informatiebeveiliging en adviseer je over de wenselijkheid en uitvoerbaarheid van nieuwe wetgeving of aanpassing van bestaande wetgeving. Bovendien bereid je de wetgeving voor en bewaak je het wetgevingstraject. Tot slot ondersteun je collega's op het dossier informatiebeveiliging bij voorkomende juridische vragen en voer je overleggen, zowel intern als interdepartementaal. Je beantwoordt Kamervragen, bereidt Kameroverleggen voor, maakt uitvoeringsplanningen voor moties en toezeggingen en bewaakt bijbehorende processen.

Als hoofd informatievoorziening zorg je voor het verder ontwikkelen en realiseren van de diensten en producten op het gebied van informatiemanagement. Je focus ligt op klantgerichtheid en innovatiekracht en je hebt een voorbeeldfunctie in het neerzetten van de gewenste organisatiecultuur. Het hoofd Informatiemanagement:

- *geeft leiding aan de afdeling Informatiemanagement met ruim 30 medewerkers;*
- *maakt resultaatgerichte afspraken met medewerkers en bewaakt en stuurt de prestaties;*
- *stuurt op verantwoordelijkheden laag in de organisatie;*
- *draagt zorg voor deskundigheidsbevordering en vraaggericht werken;*
- *bewaakt en bevordert de kwaliteit, kwantiteit en tijdigheid van de geleverde diensten;*
- *draagt zorg voor de totstandkoming van richtlijnen en procedures;*
- *draagt zorg voor de prioritering en bewaakt de uitvoering en coördinatie;*
- *draagt zorg voor de afstemming en bewaking van afdeling overstijgende vraagstukken;*
- *draagt zorg voor de integrale advisering aan management;*
- *draagt zorg voor de afstemming van managementbesluiten en vertaalt deze naar organisatorische taakstellingen en projecten en programma's;*
- *ontwikkelt en onderhoudt een relatienetwerk;*
- *initieert en bevordert samenwerking met organisaties / partijen.*

3.5.3 Functie-eisen: opleidingsniveau en competenties

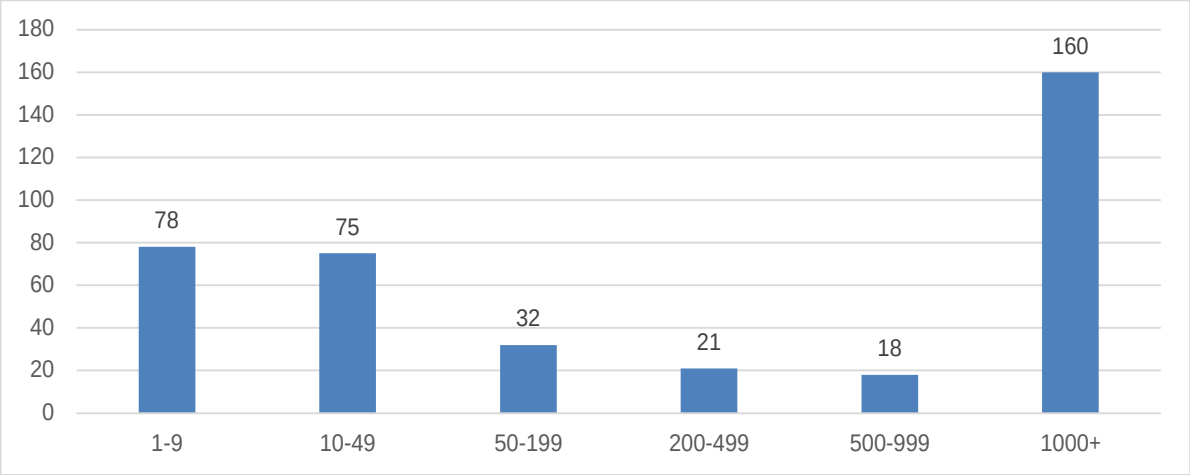
Wat betreft het gevraagde werk- en denkniveau bij niet technisch dominante functies waarbij cybersecurity een onderdeel van het werk is, zien we grote verschillen met de eerder besproken groepen. In 44% van de vacatures wordt een WO-niveau gevraagd, in 38% gaat het om HBO-/WO-niveau en in 14% van de gevallen wordt om HBO-niveau gevraagd. 4% vraagt om een HBO/MBO-niveau. Wat extra opvalt, is dat juist in operationeel-tactische functies in 50% van de gevallen om WO-niveau wordt gevraagd. Bij de andere drie groepen was dit 24% (technische dominant specialistisch, functiegroep 1), 25% (niet technisch dominant, security een onderdeel, functiegroep 2) en 16% (technisch dominant, security een onderdeel, functiegroep 3).

Als het gaat om aanvullende eisen, ontstaat een diffuus beeld. Dit komt doordat deze groep verschillende, ver uit elkaar liggende functies kent (IT auditor, manager, beleidsadviseur). Een gemene deler is de nadruk op communicatieve vaardigheden, grote mate van ervaring met name in het werkveld van de werkgever, organisatiesensitiviteit, een grote mate van conceptuele en analytische vaardigheden, en kennis van standaarden en protocollen (bijvoorbeeld ISO).

3.5.4 Profiel werkgevers

Wat bij deze functiegroep ten aanzien van andere functiegroepen anders is, is de verdeling van vacatures over branches. Niet de ICT-branche is de grootste werver van deze professionals, maar de financiële dienstverlening (17%). De ICT is verantwoordelijk voor 12% en de zakelijke dienstverlening voor 11%. Overheid (7%) en onderwijs (6%) zijn ook grote spelers. Voorbeelden van organisaties waar vacatures zijn gepubliceerd zijn Ordina, Booking.com, SoftLayer Technologies, PwC, Ziggo, CZ.[90] De grootste wervers zijn echter wel de consultancy- en detacheringsbedrijven, omdat bij deze bedrijven toch de meeste adviseurs, juridisch specialisten en auditors werkzaam zijn. In onderstaande figuur is de verdeling van vacatures naar organisatiegrootte weergegeven.

Figuur 12: Totaal aantal vacatures voor Niet technisch dominante functies waarbij cybersecurity een onderdeel is, naar organisatiegrootte (vierde kwartaal 2012 t/m derde kwartaal 2014)



Bron: PLATO op basis van vacature-analyse Jobfeed

Ook met betrekking tot deze groep, zijn het vooral de grote organisaties (meer dan 1.000 medewerkers) die verantwoordelijk zijn voor de meeste vacatures (35%). De vraag bij het kleinbedrijf is groter in verhouding tot andere groepen cybersecurityspecialisten (32%).

3.5.5 Arbeidsvoorwaarden

In 86% van de vacatures gaat het om een fulltime aanstelling, 8% betreft een parttime aanstelling en de rest kan zowel fulltime als parttime zijn. De salarisindicatie voor deze functies loopt van rond de 3.000 Euro tot 5.500 Euro (bruto, op basis van een aanstelling van 36 tot 40 uur per week). In sommige gevallen zijn functies open voor vrij ondernemerschap (zzp-ers).

3.5.6 Duiding en ontwikkeling van de vraag

Op basis van interviews met werkgevers is weinig zicht gekomen op de aanpalende beroepen. Er is een toenemende vraag naar auditors die kennis hebben van ISO-normen gerelateerd aan security en deze professionals werken voornamelijk in de zakelijke dienstverlening. Deze professionals spelen wel een steeds grotere rol in het vormgeven van beveiligingsbeleid bij bedrijven en overheden, omdat het beveiligingsbeleid veelal vormgegeven wordt aan de hand van vastgestelde procedures en eisen. Het afgeven van organisatie-brede beveiligingscertificaten wordt meer en meer verlangd door overheden (bijvoorbeeld in het kader van de nieuwe Europese Privacy richtlijn), verzekeraars en opdrachtgevers.

[90] NB: het gaat hier om voorbeelden. In het noemen van de specifieke bedrijven kan niet hun belang/belangrijkheid worden afgeleid.

Gegeven de toegenomen beleidsaandacht voor cybersecurity is het te verwachten dat ook de behoefte aan aanpalende beroepen in de toekomst toeneemt (bijvoorbeeld beleidsmakers, docenten, onderzoekers). Genoemd kan worden de gemeentelijke aandacht voor beveiliging en behoefte aan audits in het kader van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de aandacht voor privacy waarborgen in het kader van de Wet Bescherming Persoonsgegevens, en aandacht voor IT-beveiliging in initiële (informatica)opleidingen. Er is momenteel een beperkte vraag naar docenten informatica die tevens veiligheidsissues kunnen behandelen. Echter, gegeven de toename aan veiligheidsbewustzijn, mede door cybersecurity-gerelateerde incidenten, zullen ook onderwijsaanbieders in grotere mate aandacht besteden aan securityvraagstukken. Ook de vraag naar beleidsmakers met kennis van cybersecurity zal om dezelfde redenen toenemen, omdat ook op beleidsniveau de nodige initiatieven genomen moeten worden om de samenleving meer cybersecure te maken.

De verwachting is dat de vraag naar deze groep professionals (in aanpalende functies) de komende vijf jaar stijgt. Daarna wordt verwacht dat (doordat maatregelen zijn geïnitieerd om de samenleving veiliger te maken, opleidingen zijn opgezet, en bedrijven en organisaties hun security hebben georganiseerd) de vraag naar deze groep iets zal afnemen.

3.6 Afsluitende opmerkingen

We zien dat de arbeidsmarkt per functiegroep verschilt. De verschillen betreffen de functieomschrijvingen en functie-eisen in termen van gevraagde opleidingen, competenties en behaalde certificaten. Ook het profiel van de werkgevers verschilt per functiegroep wat een aanwijzing is dat het om verschillende arbeidsmarkten gaat. De arbeidsmarkt van technisch dominante cybersecurity professionals wordt gedomineerd door de consultancy en detacheringsbedrijven. Naast deze bedrijven zijn er maar weinig organisaties die een aantrekkelijk, gevarieerd werkaanbod kunnen bieden aan de professionals. In de arbeidsmarkt voor de technisch dominante functies waarin cybersecurity een onderdeel is zijn softwareontwikkelaars de belangrijkste afnemers. Echter, de 'softwareontwikkelaars' worden meer en meer een zeer gedifferentieerde groep, werkzaam in verschillende sectoren. De arbeidsmarkt van niet technisch dominante cybersecurity professionals kent een zeer gevarieerd palet aan werkgevers. Dit heeft te maken met het feit dat deze professionals, als schakel tussen techniek en organisatie, niet veelvuldig in organisaties nodig zijn. De arbeidsmarkt voor niet technisch dominante functies waarin cybersecurity een onderdeel is, kent vooral in de auditing wereld een aantal grote spelers.

Omdat het om verschillende arbeidsmarkten gaat, is het gerechtvaardigd ook discrepanties tussen vraag en aanbod en oplossingsrichtingen separaat te beschrijven (zie hoofdstuk 5).

Ten aanzien van de vestigingsplaats van de vragende organisaties, geldt voor alle functiegroepen dat veel organisaties gevestigd zijn in de Randstad (Noord-Holland, 30%; Zuid-Holland, 20%; Utrecht 15%).

De analyse van de vraag naar Cyber Security Professionals wijst op een aantal interessante aspecten van de dynamiek in de markt:

- *De markt vraagt veelvuldig om technici, terwijl dit niet altijd nodig blijkt te zijn.* Dit lijkt een symptoom van niet goed weten wat nodig is om een organisatie veilig te maken. Hierdoor wordt de oplossing gezocht in technische hulpmiddelen, tools en checklists. Echter, cybersecurity gaat veel minder over techniek dan over weet hebben van de bedrijfskundige processen en het opstellen van een risicoanalyse en dreigingsprofiel. Hierbij komt de vraag wat deze dreiging in termen van techniek betekent pas aan het einde aan de orde, niet aan het begin. Het is dit symp-

toom waarvan organisaties beter doordrongen moeten zijn. Met andere woorden, organisaties moeten beter ingelicht worden wat cybersecurity inhoudt.

- *Gebrek aan securitybewustzijn, met name bij kleinere bedrijven.* Veel kleine MKB-bedrijven zijn niet geïnteresseerd in cybersecurity. "Het overkomt ons toch niet". Men vergeet dat cybercrime zeer goed georganiseerde misdaad is: als er iets te halen valt, komen ze er vroeg of laat wel achter.
- *Cybersecurity wordt vaak als een kostenpost gezien.* Nu nog wordt beveiliging gezien als kostenpost (functionaliteit als economische meerwaarde). Dit moet veranderen en dit vraagt om een verdere ontwikkeling naar volwassenheid van de ICT-sector als geheel. Als de ICT écht volwassen wordt, kan dit betekenen dat de CSP eigenlijk niet meer nodig is: het probleem lost zich op. Gegeven bezuinigingen en reorganisaties komt cybersecurity bij een aantal organisaties onder druk te staan.
- *Krapte op de arbeidsmarkt heeft een stuwende werking op de arbeidsvoorwaarden.* Publieke organisaties kunnen vaak niet meegaan met de privaatgeboden salarissen. Aan de andere kant wordt aangegeven dat het salaris minder belangrijk is dan het takenpakket, het type klussen en de bredere organisatie waarin de CSP werkt.

De volgende trends die de vraag naar verschillende types CSP in de toekomst bepalen zijn waar te nemen:

- De toegenomen beleidsaandacht zorgt dat het beroep van CSP meer in de schijnwerpers komt te staan en dat bedrijven meer bewust worden van de kwetsbaarheid van hun ICT-systemen. Gegeven deze factoren zal enerzijds de vraag naar competente CSP's toenemen, anderzijds kunnen deze factoren een aanzuigende werking hebben op mensen die kansen zien om in deze sector werkzaam te zijn of worden (toename van het aanbod).
- Gezien de geschetste economische en bedrijfseconomische ontwikkelingen is het waarschijnlijk dat de vraag naar CSP's toeneemt. Hierbij is het de vraag hoe bedrijven in de toekomst hun IT-beveiliging organiseren en dus, welke typen CSP's nodig zijn bij welke bedrijven en organisaties.
- Burgers en overheid moeten zich meer bewust worden van de risico's, maar aangezien internet zich op alle terreinen van het dagelijkse leven manifesteert, is ook het omgaan met risico's een alledaagse bezigheid. De sociaal-maatschappelijke context laat een groeiend belang van veilige systemen zien (security by design), hierdoor neemt de vraag naar een betere balans tussen functionaliteit en veiligheid toe. Echter, omdat systemen nooit 100% veilig zijn, moeten zij ook te repareren zijn. Dit vraagt om competente CSP's.
- Verwacht kan worden dat de technologische ontwikkelingen alleen maar leiden tot een grotere vraag naar alle typen CSP's, ook in branches/sectoren waar producten momenteel nog niet 'connected' zijn.
- Wettelijke veranderingen (bijvoorbeeld Europese privacy richtlijn) hebben consequenties voor de ontwikkeling van vraag en aanbod op de arbeidsmarkt. De wetgeving vraagt meer van bedrijven en organisaties in termen van beveiliging.
- Cybersecurity is van een ICT-vraagstuk een organisatievraagstuk geworden. Dat heeft zijn weerslag op wat voor typen CSP's in de organisatie nodig zijn. Nemen bedrijven zelf mensen in dienst om de netwerksystemen te beveiligen, of maken zij gebruik van gespecialiseerde bureaus? Deze keuze bepaalt mede welke competenties een bedrijf zelf in huis moet halen (Committee on Professionalizing the Nation's Cyber Security Workforce; 2014).

Gegeven de in de vorige paragraaf geschetste ontwikkelingen t.a.v. digitalisering en de toenemende afhankelijkheid van (vitale infrastructurele) systemen, is de verwachting dat de vraag naar Cyber Security Professionals in de toekomst alleen maar zal groeien.

De grootste stijging op de middellange termijn is voorzien met betrekking tot de technische dominante functies waarin cybersecurity een onderdeel is. Dit komt doordat de

vraag naar veiligere systemen weerklinkt in de systeemontwikkeling en systeembeheersing. De vraag naar de balans tussen functionaliteit en beveiliging zal vaker aan de orde komen in de vraag naar ICT-systemen en softwarepakketten. Na een sterke groei in de eerste vijf jaar zal de vraag naar niet technische dominante cybersecurityfuncties licht dalen, doordat organisaties hun beveiliging in de organisaties hebben ingebed. Bij deze groep zal echter de vervangingsvraag tegen die tijd ook een rol gaan spelen in de ontwikkeling van de vraag omdat professionals met pensioen gaan. In vacatures zal vaker om ervaren mensen worden gevraagd.
De vraag naar specialisten voor technisch dominante specialistische cybersecurityfuncties (hackers, pen testers) zal aanhoudend stijgen. Zij delen met cybercriminelen de rol van 'front-runner' in de ontwikkeling van cybersecurity. Om de technologische ontwikkelingen op het terrein van cybercrime bij te benen, zijn in de toekomst meer van deze technisch dominante specialisten nodig. Ook de niet technisch dominante functies waarin security een onderdeel vormt zal in de toekomst meer gevraagd worden. Het cyberdomein vormt een belangrijk deel van de leefwereld en daarom zijn verschillende aanpalende functies nodig waarin kennis van cybersecurity onontbeerlijk is.

4 Aanbod van Cyber Security Professionals: onderwijs en opleiding

In dit hoofdstuk wordt allereerst ingegaan op de beschikbaarheid van informatie met betrekking tot het aanbod en deelname. Daarna worden verschillende typen (aan cybersecurity gerelateerde) onderwijs- en opleidingstrajecten in kaart gebracht en een beeld geschetst van het aantal studenten en deelnemers.

4.1 Beschikbaarheid van informatie over onderwijs en deelname

Zoals beschreven in hoofdstuk 1 (paragraaf 1.5) heeft het onderzoeksteam, naast een inventarisatie (internetresearch) en analyse van MBO-, HBO-, WO-opleidingen en opleidingen van private aanbieders, diverse vertegenwoordigers van opleidingen geïnterviewd over hun aanbod op het gebied van cybersecurity. (Zie bijlage 2 voor een overzicht van geraadpleegde onderwijs- en opleidingsinstellingen en geïnterviewden.)

De inventarisatie van het aanbod was gericht op opleidingen die georiënteerd zijn op het afleveren van specialisten in cybersecurity-gerelateerde werkvelden. Het accent lag daarbij gericht op niveaus van handelen (operationeel, tactisch, en strategisch). Het eerder gemaakte onderscheid in cybersecurity als specialisme en cybersecurity als onderdeel (in hoofdstuk 2), passen we niet rechtstreeks toe op het onderwijsaanbod. De reden hiervoor is dat een deel- of hoofdtaak in onderwijs- en opleidingen geen ter zake doend onderscheid is. Of iets nu een hoofdtaak, of een deeltaak is, de vereiste opleiding ervoor moet gelijk zijn.

Een probleem bij het vinden van cijfers is, dat de opleiding Cybersecurity als zodanig slechts in een beperkt aantal gevallen bestaat. Voor het overige zit cybersecurity als thema verweven in andere opleidingen zoals Veiligheidskunde, Informatica, Techniek en Criminologie. Daar komt bij dat de opleidingen het domein cybersecurity verschillend benaderen. Sommige opleidingen leiden Cyber Security Professionals op; andere leiden studenten op voor beroepen waarin cybersecurity een aspect of aandachtspunt is. Weer andere opleidingen houden zich wel bezig met cybersecurity, maar doen dat vanuit een specifiek ander vakgebied zoals rechtspraak of recherche. Tenslotte is cijfermatig zicht krijgen op het private aanbod en bedrijfsopleidingen (intern) enkel illustratief mogelijk. Een volledig beeld kan niet worden gegeven

Cijfermatig is de situatie intransparant te noemen. Kwalitatief ligt dat anders. Opleidingen zijn behoorlijk expliciet over wat ze te bieden hebben en in welke vorm. Met een internetsearch is goed te achterhalen welke onderwerpen in welke vorm, en in welke omvang behandeld worden. Tevens is te zien op welke doelgroepen de opleidingen zich richten. De enige uitzondering hierop vormen de bedrijfsopleidingen. Alle opleidingen die worden aangeboden in de markt hebben er belang bij zich te profileren en kenbaar te maken. Dat geldt voor open inschrijvingscursussen en ook voor uitbestede bedrijfsopleidingen. Een uitzondering vormen de interne bedrijfsopleidingen, waarbinnen interne deskundigen uit de organisatie het bedrijf het eigen personeel scholen. Dat aanbod is moeilijk te achterhalen.

4.2 Overzicht van cybersecurity-gerelateerde onderwijs- en opleidingstrajecten

In de afgelopen jaren zijn veel nieuwe opleidingsinitiatieven op het terrein van cybersecurity gestart. In het algemeen (alle initiatieven samen) is een gedifferentieerd aanbod ontstaan op verschillende niveaus, voor werkenden en studerenden; van sterk technisch gericht tot en opleidingen met een accent op integratie van verschillende invalshoeken. Er zijn technisch georiënteerde opleidingen, opleidingen die meer aandacht besteden aan de verschillende invalshoeken die een rol spelen in cybersecurity en er zijn combinatieopleidingen. Bij een aantal universiteiten en hogescholen zijn er (voor reguliere studenten) masters, specifiek op het terrein van cybersecurity. Deze masters onderscheiden zich van elkaar door de mate waarin techniek in het programma zit en de mate waarin aandacht wordt besteed aan andere invalshoeken (bijvoorbeeld: juridisch, criminologisch en/of politicologisch).

Voor professionals die al enige jaren in een managementfunctie werkzaam zijn, zijn er losse studieonderdelen toegankelijk. Deze maken bijvoorbeeld deel uit van een MBA of een executive master. Daarnaast zijn er voor CSP's tal van mogelijkheden voor het behalen van certificaten en om zich op andere manieren (bijvoorbeeld door cursussen) technisch bij te scholen.

Bij het inventariseren van het aanbod is gekeken naar verschillende functies en bijbehorende profielen. Deze zijn op twee dimensies gerubriceerd (zie figuur 2, paragraaf 2.3):

- horizontaal worden vier soorten functies onderscheiden (manager, analist, developer en support staff);
- verticaal wordt onderscheid gemaakt naar het niveau van interventie (beleidsniveau, niveau van cybersecurity, niveau van IT-security), deze verticale dimensie loopt van niet technisch dominant naar technisch dominant en van strategisch naar tactisch en operationeel.

De horizontale en de verticale indeling zijn onderscheidend maar vertonen ook samenhang. Bij ieder type aanbod wordt beschreven op welk type functies dit aanbod zich het meest richt.

Bij de inventarisatie van soorten aanbod zien we allereerst opleidingen in het reguliere onderwijs: in het middelbaar beroepsonderwijs (MBO), het hoger beroepsonderwijs (HBO) en het wetenschappelijk onderwijs (WO). Daarnaast is er een groot aanbod van particuliere opleidings- en trainingsprogramma's, gericht op professionals die al werkzaam zijn in de sector. Ook de reguliere opleidingsinstellingen (MBO, HBO en WO) bieden, naast hun reguliere aanbod, opleidings- en trainingsprogramma's aan die gericht zijn op professionals. Ten slotte is er een groot aantal ICT-bedrijven en certificerende instellingen die in de vorm van audits, korte programma's, workshops, masterclasses e.d. zich in de markt bewegen. Het aanbod van programma's gerelateerd aan cybersecurity is als volgt:

Tabel 2: Instellingen en programma's

Soorten instellingen	Aantal programma's
MBO	5
HBO	13
WO bachelor	4
WO master	12 (incl. executive masterstudies)
MBO voor professionals	1
HBO voor professionals	6
Particulier aanbod voor professionals	28
ICT-bedrijven en certificerende instellingen	12

Bron: PLATO

In bovenstaand overzicht verwijzen de aantallen naar soorten aanbod. Voor het MBO geldt dat hun aanbod op meerdere locaties worden uitgevoerd. Weliswaar hebben we vijf MBO programma's aangetroffen, maar deze worden wel op meerdere plaatsen in het land aangeboden.

In de volgende secties komen de verschillende typen aanbod aan de orde. Bij ieder type bespreken we de inhoud (richting) van de opleidingen, het aantal opleidingen en (indien voorhanden) de aantallen studenten die deze opleidingen volgen.

4.2.1 Het cybersecurity-gerelateerde MBO-aanbod

4.2.1.a Inhoud (richting) opleidingen

Het opleidingsaanbod op het gebied van ICT is groot, maar de link met cybersecurity is zwak of onduidelijk. In het MBO wordt met betrekking tot ICT onder andere opgeleid voor ICT-beheerder; netwerkbeheerder; applicatieontwikkelaar; medewerker beheer ICT; en de opleiding veiligheid en vakmanschap. Het ECABO onderscheidt ook andere (indirect) aan cybersecurity gerelateerde functies waarvoor het MBO opleidt, zoals digitaal forensisch onderzoeker; digitaal rechercheur; game developer; mediatechnoloog; en medewerker telecom. Het gaat daarom om verschillende opleidingsprogramma's. Ter illustratie volgt hieronder een voorbeeld van een cybersecurity-gerelateerde MBO opleiding 'Veiligheid en Vakmanschap', gericht op werk bij defensie.

MBO *Vakrichting ICT van de opleiding Veiligheid & Vakmanschap* *Leergang Defensie*[91]	*Studenten leren meer over het werk in een computercentrum, het installeren van ICT-apparatuur en het aanleggen van een netwerk.* *Met de vakrichting ICT kunnen afgestudeerden aan de slag bij de landmacht of de luchtmacht. Bij de landmacht gaan zij aan de slag bij de Verbindingsdienst, waar zij ervoor zorgen dat alle eenheden aangestuurd kunnen worden en met elkaar kunnen communiceren. Bij de luchtmacht gaan afgestudeerden werken bij de CIS/ICT-helpdesk, waar zij telecommunicatiesystemen, pc's en telefoonverbindingen onderhouden. Deze vakrichting dient ook een basis voor een ICT-functie in het bedrijfsleven.*

Cybersecurity zit op dit moment weinig tot niet in de ICT MBO-opleidingen. Alleen bij de opleiding tot ICT-beheerder en netwerkbeheerder wordt er enige aandacht aan geschonken, namelijk in het vak 'Informatiebeveiliging'. Er komen in 2016 echter nieuwe landelijke kwalificatiedossiers voor het MBO, waardoor er in de twee genoemde opleidingen mogelijk meer aandacht zal komen voor informatiebeveiliging en cybersecurity.

In de twee hierboven genoemde MBO-opleidingen is er dus groeiende aandacht voor een pro-actieve 'cybersecurity'-houding bij het uitvoeren van het werk als ICT-beheerder en netwerkbeheerder. Van een MBO-opleiding specifiek gericht op het voorkomen of bestrijden van cybercrime is geen sprake. Er leek enkele jaren geleden vraag naar te zijn. Daarom werd de MBO-opleiding 'Digitaal onderzoeker' (ofwel 'Digitaal rechercheur') ontwikkeld en geïmplementeerd. In de praktijk bleek het echter moeilijk om relevante stageplekken voor deze leerlingen te vinden. Stage-instellingen vonden de MBO-leerlingen te jong voor dit soort werk, omdat de digitaal onderzoeker te maken kan krijgen met vertrouwelijke informatie. Deze opleiding bestaat dan ook niet meer. In de doorstroom naar het HBO zouden security-opleidingen op MBO-3 of 4 juist nodig zijn. Dit zou bijvoorbeeld extra instroom van studenten voor het HBO op kunnen leveren.

[91] Zie: http://veva.nl/De-opleiding.html

Het aanbod in het MBO is grotendeels gericht op *ondersteunende ICT-functies* (zie figuur 13, paragraaf 4.3). Echter, in het MBO is gebleken dat het in de wat zwaardere ICT-functies moeilijk is om voor MBO-studenten stageplaatsen te regelen. Er is op de arbeidsmarkt sprake van verdringing door HBO-opgeleiden. Veel MBO'ers kiezen er dan ook voor om na het behalen van hun diploma hun studie in het HBO te vervolgen tot het niveau van associate degree, of bachelor.

4.2.1.b Kwantitatief overzicht opleidingen en studentenaantallen

Het MBO- aanbod bevat de volgende opleidingsprogramma's en aantallen aanbieders:

Tabel 3: Programma's en aanbieders

Opleidingsprogramma's	Aantallen aanbieders
ICT-beheerder	41 instellingen
Netwerkbeheerder	31 instellingen
Applicatieontwikkelaar	31 instellingen
Medewerker beheer ICT	40 instellingen
Veiligheid en vakmanschap	30 instellingen

Bron: PLATO, [1] Op basis van http://www.roc.nl/default.php

Over de ontwikkelingen van de studentenaantallen zijn, over vier van de vijf genoemde kwalificatiedossiers, instroomgegevens beschikbaar in de kennisbank van het Platform Bèta Techniek. Opgemerkt moet worden dat er van het aantal MBO studenten meer dan 40% doorstroomt naar het HBO en dus niet direct beschikbaar komt op de arbeidsmarkt.

Tabel 4: instroom MBO-studenten in verschillende cybersecurity-gerelateerde opleidingen per kwalificatiedossier

	08-09	09-10	10-11	11-12	12-13	13-14
ICT-beheerder	1.728	1.539	1.325	1.327	1.320	1603
Netwerkbeheerder	Geen gegevens beschikbaar					
Applicatieontwikkelaar	552	609	728	892	1.123	1.409
Medewerker beheer ICT	3.121	3.062	2.869	2.528	2.227	2.075
Veiligheid en vakmanschap	1.337	2.316	1.542	1.399	1.544	1.793

Bron: PLATO op basis van Platform Bèta Techniek

Uit de gegevens is te zien dat dit jaar (2013-2014) in totaal tenminste 6.880 deelnemers instromen, de niet in de kennisbank opgenomen gegevens over Netwerkbeheerder en de overige door ECABO genoemde opleidingen niet meegenomen.

Bovenstaande cijfers geven de instroom per jaar weer, cohorten dus. Het totaal aantal ingeschrevenen is daarmee natuurlijk veel hoger, namelijk minimaal het aantal cohorten maal de instroom per jaar (studievertraging kan immers voor verlenging van de inschrijfduur zorgen, en daarmee tot vergroting van de aantallen leiden). Voor de genoemde vier kwalificatiedossiers (op niveau 3 en 4) zijn er over de afgelopen zes studiejaren rond de 23 duizend studenten ingeschreven.

4.2.2 Het cybersecurity-gerelateerde HBO-aanbod

4.2.2.a Inhoud (richting) opleidingen

In het HBO worden reguliere bachelorsprogramma's aangeboden onder de volgende titels: Integrale veiligheid; Security management; Information security management; Technische informatica; Netwerk infrastructuur en design; Integrale veiligheid; ICT; ICT beheer (associate degree); Informatica en Business IT & management en de opleidingen van de Nederlandse Defensie Academie. Om een beeld te schetsen, is hieronder een voorbeeld opgenomen van een cybersecurity-gerelateerde HBO opleiding ICT.

HBO *ICT / Fontys*	*De HBO ICT opleiding is een 4-jarige bachelor opleiding. De opleiding kent 11 studieroutes waaronder[92]:* - *ICT & Business* - *ICT & Media Design* - *ICT & Software Engineering* - *ICT & Technology* - *ICT & Management and Security* - *ICT & Cyber Security* *Binnen de studieroute CT & Cyber Security wordt men opgeleid tot ICT-security-engineer en security-specialist. Na de opleiding kunnen afgestudeerden gaan werken als security engineer, security incident response engineer, security onderzoeker, security tester, netwerk- of system engineer, infrastructuur consultant, (Unix) server beheerder.*

De programma's verschillen sterk in hun focus op cybersecurity. Sommige programma's zijn ICT-gericht met security als aandachtspunt; andere programma's leggen juist het accent op veiligheid en behandelen ICT en cybersecurity als een aspect daarvan. Ook zijn er opleidingen die zich richten op informatica met cybersecurity als aandachtspunt in minors of studieonderdelen.

De aangeboden programma's tonen een veel bredere spreiding dan het MBO-aanbod. Waar we bij het MBO een focus zien op ondersteunende cyber- en IT-securityfuncties, zien we in het HBO dat het aanbod opleidt voor zowel *analisten*, *developers* als *support staff.* Bovendien is er ook een breed aanbod gericht op beleidsontwikkeling op het terrein van cybersecurity. Managementopleidingen zijn minder talrijk. Sommige opleidingen richten zich op cyber en ICT-management, of op management met een cyber- en ICT-oriëntatie. Het betreft dan management in de meer operationele zin, het gaat niet om management van beleidsontwikkeling. De accenten staan weergegeven in figuur 13, paragraaf 4.3.

4.2.2.b Kwantitatief overzicht opleidingen en studentaantallen

Net als bij de MBO-opleidingen zijn de aantallen instromers in het HBO achterhaald via het Platform Bèta Techniek. In de analyse van de daar beschikbare gegevens hebben we gezocht naar de studentenaantallen in alle studies gewijd aan information systems, information technology, math information technology and informatics, computer science, computer science and engineering, ICT, informatica, informatiekunde, information science(s), information studies, technical informatics en telematics. Van deze studies is het ICT-gehalte relatief duidelijk, maar het securitygehalte veel minder duidelijk omschreven. Er zijn weinig studierichtingen die nadrukkelijk aan cybersecurity gewijd zijn.

Tabel 5: instroom HBO-studenten in ICT/security-gerelateerde vakken

	08-09	09-10	10-11	11-12	12-13	13-14
Associate degrees	16	35	22	42	37	73
Bachelors degree	2.912	3.360	3.178	3.505	3.556	4.053

Bron: PLATO op basis van Platform Bèta Techniek

De tabel hierboven betreft de instroom. Het aantal ingeschrevenen is veel groter. Voor de bachelor degree ligt het aantal ingeschrevenen in voor CSP relevante HBO opleidingen rond de 17 duizend (2008-2012). In 2013-14 steeg dit echter naar meer dan 19 duizend.

In het HBO zien we een behoorlijke groei van de instroom over de jaren heen. Dit geldt voor zowel de associate degree studies als de bachelors degree studies. De associate

[92] http://fontys.nl/Studeren/Opleidingen/HBOICT-met-11-studieroutes-voltijd/Inhoud.htm

degree studies zijn nog pril, maar vormen voor de MBO-afgestudeerden, die in het HBO verder willen, een toegankelijk vervolg. Daarmee verschaft 40 % van de MBO'ers zich op termijn toegang tot de arbeidsmarkt.

Ten aanzien van de vraag of HBO-bachelors helemaal gericht op cybersecurity wenselijk zijn, is verschil van inzicht. Voorstanders geven aan dat hier vraag naar is, zowel vanuit studenten als vanuit organisaties. Tegenstanders benadrukken dat een stevige technische basis noodzakelijk is. De link met cybersecurity dient pas aan de orde te komen in een afstudeerproject, aparte keuzemodules of na afronding van de opleiding in het kader van bij- en nascholing.

4.2.3 Het cybersecurity-gerelateerde WO-aanbod

4.2.3.a Inhoud (richting) opleidingen

Net als in het HBO, zien we in het WO een verscheidenheid aan programma's. Er zijn opleidingsprogramma's met een directe focus op cybersecurity zoals de opleidingen van de Cyber Security Academy, studies met een meer technische of ICT-oriëntatie, zoals de master Computer Security (Kerkhoffs Instituut); studies met een accent op veiligheid en/of crisismanagement, zoals de master crisis- en securitymanagement (Universiteit Leiden); en studies met wat meer distantie tot het onderwerp, benaderd vanuit bijvoorbeeld rechtsgeleerdheid of criminologie.
De opleidingen verschillen in vorm en duur van elkaar. Er zijn volledige bachelors- en masterprogramma's die deel uitmaken van het reguliere universiteitsaanbod. Er zijn ook programma's die werkervaring als ingangseis stellen en bedoeld zijn als post-initiële masterprogramma's. Een voorbeeld betreft het IT & business programme van Neyenrode, waarin een specifiek op cybersecurity gerichte module Cyber Robustness is opgenomen en waarin het onderwerp cybersecurity in andere onderdelen meer zijdelings aan de orde komt.
Post-initiële masterprogramma's verschillen vaak in duur: 1- of 2 jarig.

Om een beeld te schetsen, is hieronder een beknopte beschrijving opgenomen van een cybersecurity-gerelateerde WO opleiding.

WO Master Information Security Technology / Universiteit Eindhoven[93] *Opleiding wordt aangeboden door een samenwerkingsverband van de TU Eindhoven, de Universiteit Twente en de Radboud Universiteit Nijmegen*	*Het gaat om een 2-jarige Master opleiding.* *De opleiding biedt de student een breed overzicht van de technieken van Information Security Technology, waarbij ook bedrijfsmatige, juridische en ethische aspecten worden betrokken. Information Security Technology laat de student kennismaken met onderwerpen als:* *cryptografische codes* *operating systemen* *protocolverificatie* *Alumni werken onder meer als intern en/of extern consultant, waarbij de veiligheid van een bedrijf of organisatie centraal staat. De volgende typen werkgevers nemen afgestudeerden aan: onderzoekslaboratoria; wetenschappelijke instellingen; Research & Development-afdelingen bij bedrijven; de financiële wereld; de consultancy wereld.*

[93] Zie: http://www.tue.nl/studeren/tue-graduate-school/masteropleidingen/information-security-technology/

Het WO aanbod van opleidingen richt zich op alle onderscheiden functiecategorieën. Dat zien we ook terug in figuur 13, paragraaf 4.3. Er wordt echter vooral opgeleid voor functies op het terrein van beleidsontwikkeling en management.

4.2.3.b Kwantitatief overzicht opleidingen en studentaantallen

De analyse van het aanbod in het WO, betreft een vergelijkbare selectie van vakgebieden als bij de analyse van het HBO-aanbod. De aantallen die aldus zijn afgeleid (zie tabel 6) betreffen de studenten die zich in de techniek, informatica of ICT bekwamen. Als we een selectie maken van studies die strikt gericht zijn op security, wordt de selectie veel kleiner. Het betreft dan twee bachelor studies (Securitymanagement en Information Security Management) en twee masterstudies (Crisis and Security Management en Law, Politics, and International Securitymanagement). Voor deze studies geldt dat onvoldoende duidelijk is wat de cybercomponent is.

Tabel 6: instroom WO-studenten in voor CSP relevante masterstudies en gerichte security studies

	08-09	09-10	10-11	11-12	12-13	13-14
Relevante Master degree	263	291	305	289	302	292
Gerichte Bachelors en masters	53	78	113	155	187	53

Bron: PLATO op basis van Platform Bèta Techniek

De figuur hierboven betreft de instroom. Het aantal ingeschrevenen is veel groter. In de voor CSP's relevante masterprogramma's gaat het ongeveer om 2,1 duizend studenten die ingeschreven staan. Met bekrekking tot de op security gerichte studies gaat het in 2013-14 om 187 studenten. Dit aantal stijgt sterk over de jaren (in 2008-09 stonden er nog maar 53 studenten ingeschreven).

Studenten ontwikkelen zich in een grote range van andere opleidingen ook op ICT-gebied. Dat geldt bijvoorbeeld voor bibliotheekopleidingen (informatiespecialist), methoden en technieken voor onderwijs, sommige delen van de lerarenopleiding, bedrijfskunde, econometrie, etc. Als gevolg daarvan is het moeilijk aan te geven hoeveel mensen er momenteel in opleiding zijn op een voor CSP's relevant terrein. Er is een groot verschil tussen het aantal direct opgeleide CSP's en het aantal in korte tijd omschoolbare professionals op aanpalende vakgebieden.

Het als bij het HBO-aanbod, bestaan er verschillen van inzicht over de mate waarin er in wetenschappelijke bachelorprogramma's aandacht moet worden besteed aan cybersecurity. Technische universiteiten vinden dat bachelorprogramma's bedoeld zijn om een stevige technische basis te leggen; een keuzemodule cybersecurity zou voldoende kunnen zijn.

Eenzelfde soort discussie is er t.a.v. de vraag of er in de breedte, of sectorgebonden aandacht moet worden besteed aan cybersecurity. In het reguliere WO-onderwijs is te constateren dat studenten sowieso minder animo hebben voor ICT-opleidingen die sectorspecifiek zijn (zie bijvoorbeeld medische informatica). Grotere bedrijven en organisaties zijn voor hun medewerkers juist wel geïnteresseerd in een sectorgericht aanbod.

4.2.4 Overig cybersecurity-gerelateerde aanbod van MBO/HBO/WO (post-initieel)

4.2.4.a Inhoud (richting) opleidingen

Behalve reguliere HBO-opleidingen hebben HBO-instellingen ook een divers post-HBO aanbod. Dat aanbod varieert enorm in aard en omvang. Onderstaand voorbeeld betreft een master class. Er zijn ook opleidingen die veel omvangrijker zijn, onder meer een cybersecurity management opleiding van 15 weken, tot en met volledige executive master programma's.

Naast de reguliere opleidingen treffen we ook een niet-regulier aanbod aan, gericht op professionals. Het niet-reguliere aanbod van de reguliere opleidingen omvat een aantal korte cursussen (Internetsecurity; Informatiebeveiliging) en daarnaast een aantal substantiëlere studies (Security management = 12 maanden; Informatica met specialisatie securitymanagement = 3 jaar). Om een beeld te geven, is hieronder een voorbeeld opgenomen van een cybersecurity-gerelateerde post-initiële HBO opleiding.

Post HBO opleiding *Masterclass Informatiebeveiliging in de zorg*[94]	*Na de opleiding weten afgestudeerden het volgende:* - *wat informatiebeveiliging is en uit welke elementen dit bestaat;* - *wat NEN 7510 inhoudt en wat deze norm voor uw organisatie kan betekenen;* - *hoe een informatiebeveiligingsbeleid moet worden opgesteld;* - *hoe een risicoanalyse voor het vaststellen van beveiligingsmaatregelen uitgevoerd kan worden;* - *hoe een cyclus voor planning en control wordt opzet;* - *de belangrijkste wetten en normen die van belang zijn bij informatiebeveiligingsbeleid.*

In het additionele aanbod, verzorgd door MBO en HBO, zien we een oriëntatie op *beleids- en managementaspecten* van cybersecurity, of juist op IT-security. Een gericht (niet regulier) opleidingsaanbod vanuit reguliere onderwijsinstellingen voor analisten en developers ontbreekt, waarschijnlijk omdat het format van zulke cursussen (kort en met heterogene doelgroepen) zich niet leent voor de diepgang die nodig is om developers en analisten op te leiden.

4.2.4.b Kwantitatief overzicht opleidingen en studentaantallen

Het aantal deelnemers aan de post-initiële opleidingen, aangeboden door HBO en WO, blijkt substantieel. Drie opleidingen op HBO niveau, waar interviews zijn gehouden, melden gezamenlijk 650 deelnemers aan hun sterk op cybersecurity gerichte opleidingen. De opleidingen melden ook internationale samenwerking. Daarin liggen kansen voor instroom vanuit het buitenland naar de nationale markt, maar natuurlijk ook andersom een gang van Nederlandse studenten naar arbeid in het buitenland.

4.2.5 Het cybersecurity-gerelateerde private aanbod van opleidingen en trainingen gericht op professionals

4.2.5.a Inhoud (richting) opleidingen

Het private aanbod is zeer divers. Er zijn opleidingen die gericht zijn op speciale beroepsgroepen. The Academy of European Law biedt speciale opleidingen voor rechters en aanklagers. Nijenrode biedt naast een veelheid van ander aanbod ook eendaagse masterclasses voor professionals in het bedrijfsleven en publieke organisaties. Er zijn instituten die een hele range van korte cursussen aanbieden op diverse terreinen.[95] Ook gaat

[94] Zie: http://www.inholland.nl/Academy/Opleidingen/Zorg+Welzijn+en+Publieke+Dienstverlening/Management+bedrijfsvoering+ICT+en+HRM/Informaiebeveiliging+in+de+zorg/Frontpage.htm

[95] Zoals: Cloud Security (CCSK); Cloud Security, Audit en Compliance (CSAC); CISSP Compact Training (5-dagen / Engelstalig); CISSP Training (11-dagen / Nederlandstalig); Certified Ethical Hacker (CEH); Computer Hacking Forensisch Onderzoeker; ISO 27001 Lead Implementer; ISO 27001 Lead Auditor; ISO 27001 Certificering; CISA; CISM; Information Security Management; Penetration Testing Advanced; SABSA Foundation; SABSA Advanced; Security Analyst & Licensed Penetration Tester (ECSA/LPT); IT Security Architectuur; Information Security Management Professional; Digitaal Forensisch Onderzoeker.

het om schriftelijke certificerende cursussen.[96] Naast het geschetste aanbod, en vaak ook ermee verweven, zijn er allerlei systemen en certificaten (zie tekstbox).

Certificaten (niet een uitputtend overzicht):
- *CISSP - Certified Information Systems Security Professional, Practitioner, Auditor, Manager (ISO gecertificeerd) en ISFS (Information Security Foundation)*
- *CCNP Security - Cisco Certified Network Professional*
- *CISM - Certified Information Security Manager*
- *SSCP - Systems Security Certified Practitioner*
- *CAP - Certified Authorization Professional*
- *CSSLP - Certified Secure Software Lifecycle Professional*
- *SABSA - Sherwood Applied Business Security Architecture*

Toetsende/certificerende organisaties zijn onder meer EXIN Utrecht en ISACA - Information Systems Audit and Control Association.

Opleidingen worden aangeduid met de volgende namen: Information security management; Network security professional; Information security experts; Certified ethical hacker; Digital forensic analysis professional; Business continuity management professional; Penetration tester; Computer hacking forensic investigator; Auditor informatie beveiliging; Digitaal rechercheren; Identity and access management; Anti fraude professional; Informatiebeveiliging in de zorg; Data governance en data kwaliteit voor solvency; Executive master of IT auditing.

De genoemde opleidingen betreffen doorgaans korte cursussen variërend van één dag tot honderd dagen, of in het geval van de genoemde executive master dertig maanden. Voor veel aanbod geldt dat er meerdere aanbieders zijn. Dat betekent dat het volume van de geboden opleidingen dus veel groter is dan op grond van de inventarisatie van soorten aanbod het geval lijkt te zijn.

Ter illustratie zijn hieronder twee voorbeelden opgenomen van cybersecurity-gerelateerde private opleidingen.

Certified Ethical Hacker (CEH)[97] *Verschillende aanbieders*	*De 5-daagse CEH training is bedoeld voor: systeem- en netwerkbeheerders, applicatiebeheerders, webbeheerders, IT managers, Security managers en IT auditors die de beveiligingsproblematiek offensief willen aanpakken door te leren denken en werken als een hacker. Deze training is ook voor technisch management zeer interessant.*
Business Continuity Management Professional (BCMP)[98] *Verschillende aanbieders*	*Post-HBO diploma en voor de officieel geregistreerde titel BCMP. Het betreft een 16 daagse opleiding (incl. examendag). De opleiding Post-HBO Business Continuity Management Professional is geschikt voor zowel technici als managers en is vooral bestemd voor de: Business Continuity Manager; Facility Manager; BHV Manager; Operations Manager; Risico Manager; Security Manager; ICT Manager; QA/QC, KAM of Kwaliteitsmanager; Controller.*

[96] Op terreinen als: CISSP; CRISC (Certified in Risk and Information Systems Control); Identity Management & Access Control; Informatiebeveiliging; Internet Security.
[97] Zie bijvoorbeeld: http://www.computrain.nl/cursus/Certified-Ethical-Hacker-CEH-Version-8-312-50CEHV8.html
[98] Zie: https://www.securityacademy.nl/opleidingen/opleiding-post-hbo-bcm-professional.html

Anders dan in het commerciële aanbod van instellingen voor hoger onderwijs is het aanbod in de private sector behoorlijk gespreid. Er is relatief veel aanbod voor *cybersecurity en IT-securityanalisten*. Tevens is er veel aanbod voor *beleidsmedewerkers*. Ook in deze vorm van aanbod zijn de aantallen opleidingen voor developers relatief klein. Dat vergt wellicht eerder een uitgebreider programma dan de dikwijls wat kortere cursussen die particulier worden aangeboden.

4.2.5.b Kwantitatief overzicht opleidingen en studentaantallen

Cijfers over de deelname aan particuliere opleidingen en certificeringtrajecten zijn nauwelijks beschikbaar. In interviews kwam naar voren dat er minder animo is die gegevens te verstrekken. Wel wordt er telkens een groei vermeld. Dat geldt enigszins voor de particuliere aanbieders, maar nog sterker voor interne bedrijfsopleidingen. Uit de interviews blijkt dat respondenten, ondanks de kwantitatieve intransparantie, per saldo groeiende studenten- en deelnemersaantallen waarnemen. Landelijke analyses van studiekeuzes laten zien dat bètavakken een toenemende populariteit genieten, ook en vooral toenemend onder meisjes. Onduidelijk is in welke mate dat de ICT-opleidingen betreft, of nog meer in het bijzonder cybersecurity-opleidingen.

4.3 Duiding van het aanbod en overstijgende kwesties

Op basis van de inventarisatie van het opleidingsaanbod en interviews met opleidingsinstellingen is een beeld ontstaan van de veelheid aan typen onderwijsaanbod op het terrein van cybersecurity. In onderstaand overzicht is weergegeven welk type aanbod zich richt op welke functies.

Figuur 13: Type aanbod naar functies

Onderwerp ↓	Managers	Analisten	Developers	Support staff
Cyber risicobeleid	Vooral WO	HBO WO privaat	HBO WO privaat	HBO WO privaat
Cybersecurity (cyber risico-inschatting en –beheersing)	WO/HBO/ Privaat	HBO/WO/ privaat	Vooral HBO/WO	Vooral HBO
IT-security (IT risico-inschatting en –beheersing)	Vooral privaat	Vooral privaat	HBO WO privaat	MBO HBO WO privaat

In deze paragraaf duiden we de veelheid aan trajecten en reflecteren we op type-overstijgende kwesties.

4.3.1 Een rijk en gedifferentieerd cybersecurity-gerelateerd aanbod

Het aanbod aan opleidingen is inhoudelijk rijk. Er zijn *veel aanbodvarianten*[99] *en een groot aantal aanbiedingslocaties*. Dat geldt zowel voor het aanbod op MBO-niveau, als ook voor het hoger onderwijsaanbod en de particuliere programma's. We hebben ruim tachtig soorten aanbod geïnventariseerd, maar als we het aantal aanbiedingslocaties daarin verwerken dan gaat het om vele honderden opleidingen en andere vormen van aanbod. De opleidingen worden op talrijke locaties aangeboden. Dat maakt dat de opleidingen in de omgeving van de geïnteresseerden te vinden zijn. Dat geldt in het bijzonder voor het MBO- en HBO-aanbod, in iets mindere mate voor het WO, maar weer in hoge mate in de particuliere opleidingswereld.

[99] Een poging tot categorisering levert het volgende beeld op: initiële opleidingen; post-initieel onderwijs; korte cursussen; masterclasses; workshops; seminars; on the job leren; afstandsonderwijs; in-company training.

Aan de vele verschillende opleidingsvormen liggen verschillende overwegingen ten grondslag:

- De behoefte aan het leggen van een stevige technische/ICT-basis krijgt vorm in initiële opleidingen van langere duur (associate degree, bachelor en master).
- Specialisatie op het terrein van security of deeldisciplines die daarmee samenhangen, krijgt vorm in post-initieel onderwijs, waarvoor vaak ervaringsjaren als entree-eis gelden.
- Korte cursussen zijn meestal gericht op specifieke werkgerelateerde ICT- en cyber kwesties, werkwijzen en tools, vaak deel uitmakend van gecertificeerde werkprocedures.
- Masterclasses zijn korte bijeenkomsten waarin in korte tijd gewerkt wordt en kennis gedeeld wordt rond bewustzijn en strategieën met betrekking tot. cybersecurity.
- Workshops worden ingezet als er meer *hands on* training nodig is. 'Hackersworkshops' zijn daarvan een voorbeeld.
- Seminars zijn bedoeld om nieuwe inzichten te verspreiden onder beroepsgenoten.
- Afstandsonderwijs: Met computers is het leren gemakkelijk dicht bij het werk te brengen, dat geldt ook voor schriftelijk studiemateriaal/werkmateriaal. Leren op de werkplek en leren met collega's wordt mogelijk door middel van afstandsonderwijs en schriftelijk studiemateriaal. Het doel van dergelijke werknabije aanpakken is het transferprobleem van de opleiding naar het functioneren in het werk op te lossen of te verkleinen.

Uit de inventarisatie van het opleidingsaanbod blijkt dat het aanbod per opleidingsniveau en soort aanbieder weliswaar verschilt, maar dat het aanbod in zijn geheel alle functies lijkt te bedienen. Het MBO richt zich in het bijzonder op ondersteunende ICT functies. Het HBO richt zich in zijn initiële opleidingsaanbod op alle soorten functies met uitzondering van de functie manager cyberrisico beleid. Het WO bereidt voor op alle onderscheiden functiesoorten. Dat geldt ook voor de private aanbieders. Voor elk type functie is een privaat aanbod beschikbaar.

De opleidingen laten een grote variatie in inhoudelijke invalshoeken zien: technisch; informatica; criminologie; veiligheidskunde; ICT; cybersecurity; informatiemanagement; crisisbeheersing; software development; recherche; forensisch onderzoek; penetratietesten; projectmanagement, systeembeheer. Wat hierin opvalt, is dat het reguliere aanbod wat meer op algemene ICT, informatica, en cyberkennis gericht zijn, terwijl het op professionals gerichte aanbod en het particuliere aanbod voor professionals veel specifieker op IT- en cybersecurity ingaat.

In de cijfers over deelname aan opleidingen in het MBO, HBO en WO zien we op onderdelen snelle fluctuaties in studiekeuze, zoals de plotselinge groeiende belangstelling voor gaming en apps-development. Dat geeft een beeld van een *snelle adaptieve markt*, waarin snel op optredende opleidingsbehoeften wordt gereageerd. De vraag is echter of de opleidingswereld hierbij reageert op de behoeften uit de arbeidsmarkt, of op de behoeften uit de opleidingsmarkt, namelijk het werven van studenten door middel van aantrekkelijke opleidingen, ongeacht of daarvoor een arbeidsmarktperspectief is.

4.3.2 Type- en aanbod overstijgende kwesties

In de interviews kwamen ten aanzien van de invulling van het aanbod de volgende kwesties naar voren:

- *Docenten/aansluiting praktijk:* In het onderwijs is de aansluiting met de praktijk essentieel. Er wordt veel gewerkt met gastdocenten uit bedrijven of overheidsorganisaties. Ook zijn er werkveldcommissies die meekijken naar doelen, eindtermen en in te brengen cases. Bij WO-bachelors en -masters worden docenten betrokken met een WO-achtergrond. Bij HBO-bachelors en –masters en bij MBO-

opleidingen is dat niet altijd zo. Daar wordt ook gewerkt met docenten die ICT-ervaring in de praktijk hebben en daarover veel kunnen vertellen en laten zien.

- *Spanningsveld kennis en vaardigheden studenten/docenten:* Het actuele deskundigheidsniveau van docenten in de niet cybersecurity specialistische opleidingen is een probleem. Dit speelt zowel op HBO-als op WO-niveau. Studenten weten en kunnen soms meer dan docenten. Docenten moeten zich voortdurend bijscholen. Het besef groeit dat docenten meer de rol moeten spelen van het organiseren en creëren van een leeromgeving waarin mensen van elkaar leren. Dit probleem is niet van toepassing op de specialistische cybersecurity-opleidingen.
- *Focus van de opleidingen verschuift:* Opleidingen kunnen zich niet meer alleen richten op het *secure* maken van systemen. Het is ook van belang te werken aan een veerkrachtig(e) organisatie en systeem (een incident snel te boven zijn) en je profileren op het vlak van preventie en *competitive intelligence*. Ook bewustzijn van risico's en het voorkomen daarvan is belangrijk. Dit moet een plek krijgen in alle opleidingen; niet alleen in de zin van 'hoe bewust ben ik zelf?', maar ook 'hoe maak ik anderen (zoals collega's en klanten) bewust?'
- *Opleidingen uitbreiden of (nog) niet?* Veel opleidingen geven aan dat er nu een palet is van elkaar niet of minimaal concurrerende opleidingsmogelijkheden. Veel initiatieven zijn pas onlangs gestart. De wens vanuit opleidingen is om eerst te bezien hoe deze opleidingen, de studentenaantallen en de vraag van organisaties zich ontwikkelen. Er zijn geluiden dat er vanuit bedrijven en publieke organisaties een grotere vraag is, maar dat zien opleiders nog niet terugkomen in vacatures die specifiek betrekking hebben op cybersecurity.
- *Aantrekkelijkheid:* Cybersecurity is voor studenten (net als apps development en gaming) een 'sexy' onderwerp. Ze vinden dit interessant, het motiveert hen. Dit gegeven gekoppeld aan het feit dat studenten zich in hun studiekeuze snel aanpassen aan nieuwe uitdagingen en mogelijkheden, versterkt de aansluiting met de arbeidsmarkt. In interviews met I(C)T-opleidingen op MBO-, HBO- en WO-niveau wordt benadrukt dat er veel animo is voor hun opleidingen. Het aantal instromers is de afgelopen 4 á 5 jaar toegenomen. Nagenoeg iedereen die een baan zoekt, vindt er een.
- *Basis en verdieping:* De ontwikkelingen volgen elkaar snel op, waardoor er telkens nieuwe risico's, beveiligingsmogelijkheden en -middelen ontstaan. Zo bezien lijkt de cyberwereld enorm dynamisch en nauwelijks voorspelbaar. Daar tegenover staat echter dat vanuit de opleidingen een pleidooi wordt gehouden voor een stevig fundament in ICT, informatica en techniek. Het is pas bovenop dat fundament dat de CSP zich door middel van korte en flexibele vormen van opleidingsaanbod en leerarrangementen aanvullend kan scholen en ontwikkelen.
- *Overzicht cursussen:* Er zijn veel websites van opleidingen, en sites die hulp bieden bij het zoeken van opleidingen. Het overall beeld toont niettemin veel intransparantie.

5 Discrepanties op de arbeidsmarkt en oplossingsrichtingen

In hoofdstuk 3 en 4 zijn de vraag- en aanbodzijde van de arbeidsmarkt in kaart gebracht. Hoofdstuk 3 beschreef de vraag naar verschillende CSP's aan de hand van overzichten van vacatures en in hoofdstuk 4 kwam het opleidingsaanbod van opleidingen gerelateerd aan CSP's aan bod. In dit hoofdstuk confronteren we vraag en aanbod en kijken we naar discrepanties op de arbeidsmarkt en mogelijke oplossingsrichtingen.

Gevonden discrepanties en oplossingsrichtingen zijn besproken in een bijeenkomst met experts. De verkregen inzichten zijn in dit hoofdstuk geïntegreerd weergegeven (zie ook hoofdstuk 1, paragraaf 1.5 en bijlage 3).

5.1 Inleiding model discrepantieanalyse: relateren vraag en aanbod

We vertrekken vanuit de op basis van dit onderzoek (in hoofdstuk 2) vastgestelde *vier functiegroepen:*

- Technisch dominante specialistische cybersecurityfuncties (functiegroep 1).
- Niet technisch dominante specialistische cybersecurityfuncties (functiegroep 2).
- Technisch dominante functies waarbij cybersecurity een onderdeel is (functiegroep 3).
- Niet technisch dominante functies waarbij cybersecurity een onderdeel is (functiegroep 4).

Deze groepen relateren we aan het aanbod van professionals dat van initiële opleidingen komt en via andere routes werkzaam raakt als CSP.

Onderwijs speelt een belangrijke rol, maar de relatie tussen onderwijsprogramma's en de typen CSP's is vaak ondoorzichtig. Bij een arbeidsmarktonderzoek naar een beroep als bijvoorbeeld logopedist, is het vrij duidelijk naar welke vacatures er gezocht moet worden en welke opleidingen mensen opleiden voor de gevraagde posities. Voor dit beroep is voorzien in een beroepsprofiel en beroepstaken zijn duidelijk omschreven. Hierdoor is ook de opleiding helder te bepalen en te beschrijven. Hoe anders is dat in het geval van Cyber Security Professionals. In hoofdstuk 2 en 3 is uitvoerig beschreven hoeveel verschijningsvormen er van het beroep bestaan. Ook aan de opleidingskant is die spreiding zichtbaar. Het aantal specifiek op cybersecurity gerichte opleidingen is klein, maar daaromheen zijn er talrijke soorten opleidingen die direct of indirect kwalificeren voor cybersecurityfuncties.

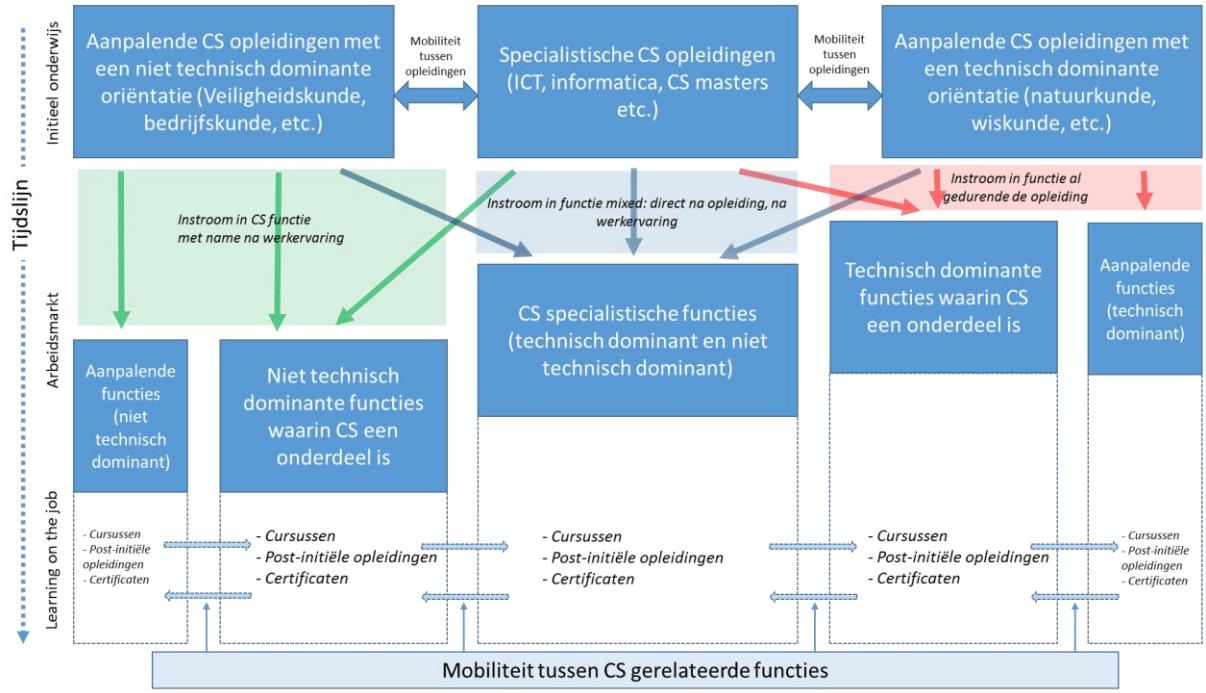
De range van opleidingen bestrijkt allereerst een grote variëteit van opleidingen met duidelijke technische componenten, en informatica-inhouden. Daarnaast zijn er opleidingen met duidelijke veiligheids-, juridische, of forensische inhouden. Ten slotte zijn er veel opleidingen die deelnemers indirect, maar diepgaand scholen in voor cybersecurity relevante vakken en competenties. In die categorie vallen opleidingen met een sterke ICT-component, maar die gericht zijn op andere dan technische- of veiligheidsgebieden, zoals kunstmatige intelligentie, studies methoden en technieken, medische informatiekunde, logistiek, meet- en regeltechniek, etc. Al met al is er een veel breder aantal opleidingen dat aan de kennis en kunde van studenten/deelnemers bijdraagt, dan alleen de direct op ICT-, of internet- en cybersecurity gerichte opleidingen.

Tot zover bespraken we de aansluiting van vraag en aanbod op de arbeidsmarkt voor CSP's in termen van afstemming van de vraag naar CSP's vanuit organisaties en het

aanbod vanuit onderwijs en opleidingen. De werkelijkheid is veel complexer dan dat. Veel studenten of opleidingsdeelnemers betreden de arbeidsmarkt al voordat ze hun studie voltooien. Anderen betreden de arbeidsmarkt, maar niet direct in een cybersecuritypositie. Zij gaan bijvoorbeeld werken in een technische ICT-functie en ontwikkelen daar hun competenties tot een niveau waardoor ze gevraagd worden voor cybersecurityfuncties in hun organisaties, omdat ze zich bekwaam hebben getoond in hun technische ICT-werk. Daarnaast zijn er professionals die in hun werk hun talenten laten zien en zich via scholing en cursussen voorbereiden op een loopbaanstap op het terrein van cybersecurity. Zij belanden pas na verloop van tijd in cybersecurityfuncties.

Gezien de snelle ontwikkelingen in de Cybersecurity wereld, is een dergelijk patroon van opgeleid worden, werken, leren op de werkplek (inclusief de virtuele kant ervan), bijgeschoold worden, loopbaanontwikkeling etc. eerder regel dan uitzondering. Dit geldt overigens ook voor veel andere sterk aan verandering onderhevige beroepen. Dat alles wordt nog versterkt door de steeds nauwer sluitende regelgeving, waardoor organisaties en bedrijven zich via certificering op allerlei punten moeten verantwoorden. Om daartoe in staat te zijn, volgen professionals geregeld cursussen om te leren via welke werkwijzen, hardware en software ze (internet)veiligheid kunnen vergroten en aantonen. Daardoor ontstaat er een uitgebreid stelsel van opleidings- en leerroutes die bijdragen aan de actualisering en upgrading van het cybersecuritywerk.

Figuur 14: Overzicht leerroutes en transitie van opleiding naar arbeidsmarkt



In bovenstaand schema staan allerlei routes aangegeven die doorlopen kunnen worden in de opleidingen en daaropvolgende leertrajecten. Het geeft een dynamisch beeld. Studenten starten hun opleiding en komen op een bepaald moment op de arbeidsmarkt. Dat moment valt dikwijls al eerder dan de afronding van de studie. Sommigen komen direct in cybersecurityfuncties, maar velen bereiken die functies pas na opbouw van ervaring in aanpalende functies of krijgen in eerste instantie functies waarin cybersecurity een onderdeel van het takenpakket is. Daarna volgt er (via processen van verder leren op de werkplek, arbeidsmobiliteit en aanvullende scholing) een verdere loopbaanontwikkeling die mogelijk in de richting van cybersecurity gaat. Een groep van professionals gaat later in de loopbaan opnieuw aan de studie, bijvoorbeeld door deel te nemen aan een professionele master of ander masterprogramma op het terrein van cybersecurity of daarvoor relevante vakgebieden. Die route is in bovenstaand schema weergegeven door te verwij-

zen naar 'post-initiële opleidingen'. Hierin kan een overlap bestaan met het initiële aanbod (bachelor- en masteropleidingen). Deze post-initiële opleidingen betreffen vaak programma's die jaren van ervaring als instroomeis stellen. Op de leerroutes per functiegroep wordt in het vervolg van dit hoofdstuk afzonderlijk ingegaan. Daarbij bespreken we ook telkens de discrepanties die we constateren in de arbeidsmarkt voor de onderscheiden groepen.

De *discrepanties* op de korte en middellange termijn tussen vraag en aanbod kunnen van de volgende aard zijn (zie hoofdstuk 2):

- Van *kwantitatieve discrepanties* is sprake wanneer er voor de cybersecuritysector ofwel te weinig (gediplomeerde) schoolverlaters en andere categorieën werkzoekenden zijn, dan wel er voor deze werkzoekenden (gediplomeerden, werkloze werkzoekenden, baanwisselaars) te weinig vacatures zijn.
- *Kwalitatieve discrepanties* treden op wanneer de technisch-instrumentele eisen en/of sociaal-normatieve eisen van de werkgevers in de cybersecuritysector hoger zijn dan de kennis, kunde, competenties en/of sociale vaardigheden[100] van (gediplomeerde) schoolverlaters en andere categorieën werkzoekenden, dan wel wanneer deze werkzoekenden hogere eisen stellen aan arbeidsinhoud, -voorwaarden en -omstandigheden dan wat werkgevers binnen de sector willen/kunnen bieden.
- Ten slotte kan sprake zijn van *ondoorzichtigheid (ofwel intransparantie)* van de arbeidsmarkt van de cybersecuritysector. Dan gaat het vooral om verschillen tussen het wervingsgedrag van de werkgevers en het zoekgedrag van (gediplomeerde) schoolverlaters en andere categorieën werkzoekenden. De mate waarin bepaalde groepen werkzoekenden voor werkgevers in beeld komen en het imago van het beroep en de sector kunnen hierbij een grote rol spelen.

Daarnaast kan er sprake zijn van discrepanties, die niet zozeer de vraag en het aanbod confronteren, maar breder van aard zijn, zoals een discrepantie tussen het belang van cybersecurity en het bewustzijn bij bedrijven voor cybersecurity.

De *oplossingsrichtingen* die in dit hoofdstuk naar voren komen zijn mede gebaseerd op interviews met deskundigen en een bijeenkomst met experts die in de afrondende fase van dit onderzoek is gehouden (zie bijlage 3). In zijn totaliteit was hierbij cybersecurity-expertise vanuit organisaties in het publieke en private domein (waaronder tevens onderwijsorganisaties) vertegenwoordigd. De oplossingsrichtingen zijn enerzijds gelinkt aan de discrepanties per functiegroep, anderzijds worden zogenaamde transversale oplossingsrichtingen onderscheiden (functiegroepdoorsnijdend en -overkoepelend). Het genereren van oplossingsrichtingen in dit onderzoek betrof vier domeinen:

1) Aanpassen van bestaand initieel onderwijs;
2) Scholing van werkenden (post-initieel opleiden);
3) Doorvoeren van veranderingen in de werkprocessen van organisaties, waarbij het kan gaan om het verplaatsen van activiteiten, veranderen van arbeidsvoorwaarden en het aantrekken van mobiele personen (internationaal werven).
4) Alternatieve maatregelen om expertise in het veld te vergroten en te benutten.

In interviews en de expertmeeting werd benadrukt dat de oplossing zal bestaan uit een mix van instrumenten die effect hebben op de korte en (middel)lange termijn. Enkel inzetten op instrumenten die op de lange termijn effect hebben, geeft geen oplossing op korte termijn en leidt mogelijk tot negatieve varkenscycluseffecten (overschotten en tekorten lossen elkaar af)[101].

[100] Naar: Van Hoof, J.J. Dronkers, J. (1980). Onderwijs en arbeidsmarkt, een verkenning van de relaties tussen onderwijs, arbeidsmarkt en arbeidssysteem.
[101] Zie onder anderen: Bouman, A., Varkenscycli op de arbeidsmarkt, Economisch Statistische Berichten, 23 augustus 1989.

5.2 Discrepantieanalyse per functiegroep

In hoofdstuk 3 is een beeld geschetst van de vier CSP-profielen op basis van literatuuronderzoek, vacatureteksten en interviews met werkgevers en professionals. Uit de *vacature-analyse* kwam naar voren dat er op jaarbasis in 2014 ongeveer 1.160 vacatures gepubliceerd worden voor cybersecurity-gerelateerde functies. Uit de *omgevingsanalyse* blijkt dat door politieke, economische, sociale, technologische en juridische ontwikkelingen de vraag naar CSP's in de toekomst zal toenemen (zie hoofdstuk 1 en 2). Zo breidt het cyberdomein zich meer en meer uit en zien we softwaretoepassingen op zo mogelijk alle domeinen van menselijk handelen terugkomen (internet of things). Belangrijk is ook de in hoofdstuk 3 beschreven trend van "extrapolisering" van de arbeidsmarkt. Prognoses duiden erop dat de vraag naar hoger en lager opgeleiden stijgt, terwijl die naar middelbaar opgeleiden daalt. Sociale competenties (communicatief, teamwork, leiding geven, verantwoordelijkheid nemen, etc.) van die hoger opgeleiden worden in toenemende mate belangrijk gevonden. Dat geldt voor functies in alle sectoren, ook voor cybersecurityfuncties. De risico's en impact van cybercriminaliteit zullen de komende jaren alleen maar toenemen. Ook worden bedrijven zich meer en meer bewust van het feit dat cybersecurity niet alleen een ICT-issue is, maar een integraal thema. Cybersecurity is van een ICT-vraagstuk een 'boardroom issue' geworden, want het voortbestaan van het bedrijf kan in het geding komen. Deze ontwikkelingen bevorderen de vraag naar alle typen CSP's.

Wat betreft het *opleidingsaanbod*: In hoofdstuk 4 kwam naar voren dat de volgende aantallen mensen in een relevante vooropleiding zitten:

- een instroom van 6.880 deelnemers op MBO 4 niveau;
- een instroom van 73 deelnemers op HBO associate degree niveau;
- een instroom van 4.053 deelnemers op HBO niveau;
- een instroom van 292 deelnemers op Master niveau;
- een instroom van deelnemers aan post-academische/post-executive masters van (blijkens de interviews) zeker 200 personen.

De genoemde aantallen zijn groot in vergelijking met het aantal gepubliceerde vacatures. Er is dus een groot potentieel aan mensen die in principe inzetbaar lijken. De getallen zijn instroomaantallen, dus we moeten incalculeren hoeveel studenten onderweg uitvallen, vertraging oplopen of andere keuzes maken dan voor het beroep van CSP. Maar zelfs als we die uitval op 50% schatten, blijven de aantallen nog hoog in vergelijking met de beschikbare vacatures. De recent uitgebrachte Keuzegids voor het hoger onderwijs concludeert dat de baankansen voor informatici relatief klein zijn. Als argumentatie wordt aangevoerd dat informatici veelal jong zijn en dat er derhalve weinig van hen uitstromen vanwege het bereiken van het einde van hun loopbaan. Een en ander is gebaseerd op studies van het Researchcentrum Onderwijs en Arbeidsmarkt (ROA).[102] Omdat voor de cybersecurity juist (sociaal vaardige) HBO'ers (en soms MBO-4 opgeleiden) nodig zijn, lijkt een scenario van krapte voor dit segment van de ICT het meest waarschijnlijk. De constatering van werkgevers dat men moeilijk aan personeel kan komen bevestigt dit ook. De Intelligence Group meldt dat 44% van de ICT'ers maandelijks wordt benaderd door een recruiter (ICT-arbeidsmarktmonitor 2014)[103].
Echter, velen van hen kiezen voor een andere inzet van hun expertise dan in de cybersecurity. De opgave lijkt niet zozeer te zijn om meer mensen op te leiden, maar veeleer om hen tijdens hun opleiding te interesseren voor cybersecurity en voor banen in die sector. De aansluitingsproblemen (discrepanties tussen vraag en aanbod) die in bedrijven en organisaties worden ervaren, zijn eerder van kwalitatieve dan van kwantitatieve aard of te wijten aan intransparantie van de arbeidsmarkt. In het vervolg van dit hoofdstuk

[102] De arbeidsmarkt naar opleiding en beroep tot 2018, ROA-R-2013/11, Researchcentrum voor Onderwijs en Arbeidsmarkt, Maastricht University School of Business and Economics Maastricht, december 2013

[103] Zie: http://www.intelligence-group.nl/nl/actueel/downloads/ict-arbeidsmarktmonitor-2014#collapseForm

wordt nader ingegaan op de situatie voor de afzonderlijke functiegroepen. Per functiegroep komt aan de orde:

a) kenmerken van de functiegroep;
b) opleidingsroutes gerelateerd aan deze functiegroep;
c) discrepanties op de arbeidsmarkt;
d) oplossingsrichtingen.

5.2.1 Technisch dominante specialistische functies (functiegroep 1)

Dit betreft functies die zeer specifiek op IT/informatiebeveiliging gericht zijn, waarbij de technische component een grote rol speelt. Daarbij kan het ook gaan om aansturende functies, waarbij een hoog-technische achtergrond vereist is. Voorbeelden zijn: ethical hackers, penetratie-testers, software testers en technical security engineers.

5.2.1.a Kenmerken van de functiegroep

In deze functiegroep gaat het vaak om zeer specialistische kennis en vaardigheden. Veelal hebben professionals die werkzaam zijn in deze functies al veel ervaring (dit kan beroepsmatig, maar ook hobbymatig zijn). De term 'startersfunctie' is niet echt van toepassing op deze functiegroep, aangezien veel mensen die in deze functies rollen al dan niet professioneel ruime ervaring hebben met programmeren en security. Ze weten wat ze waard zijn op de arbeidsmarkt en willen vooral interessant werk doen. Dit vertaalt zich ook naar een groep professionals die hun diensten als zzp-er aanbieden bij verschillende organisaties. Hierbij gaat het om professionals met zeer specialistische kennis van systemen, programmeertalen of veiligheidsaspecten.

Hieronder is een profiel weergegeven van een typische professional in deze functiegroep.

Hans is 26 jaar en is al van jongs af aan geïnteresseerd in programmeren. Op zijn 13de bouwde hij zijn eerste website en sindsdien heeft hij voor veel kennissen, vrienden, en vrienden van kennissen klusjes gedaan. Naast het bouwen en programmeren begon hij als 16-jarige ook te kijken naar waar gaten zitten in systemen. Op internetfora struinde hij rond en kwam hij in contact met mensen met soortgelijke interesses.

Ondanks dat hij geen goede leerling was (eigenlijk interesseerde het hem allemaal niet zo), kon hij een hbo-opleiding Informatica volgen. De inhoud van de opleiding viel hem tegen en pas toen hij in het tweede jaar stage ging lopen werd hem duidelijk dat, ondanks dat hij veel technische kennis en vaardigheden had, hij echt moest werken aan zijn communicatieve vaardigheden.

Al voordat hij zijn opleiding had afgerond had Hans van een aantal bedrijven een baan aangeboden gekregen. Hij koos uiteindelijk voor een bedrijf, gespecialiseerd in cybersecurity. Het salaris was lager dan dat de andere bedrijven hadden geboden, maar Hans had het idee dat hij hier het meest kon leren. Hans voerde penetratietesten uit en keek bij opdrachtgevers of de ICT-systemen veilig zijn.

Hans volgde een aantal interne opleidingen en haalde een aantal certificaten. Nadat hij drie jaar in dienst was, ging hij in op een aanbod van een grote financiële instelling, waar hij momenteel werkzaam is als analist binnen een team van ongeveer tien analisten.

5.2.1.b Opleidingsroutes gerelateerd aan deze functiegroep

De opleidingsachtergrond van mensen werkzaam in deze functie is veelal technische ICT. Specialisten die van een initiële cybersecurity-opleiding komen zijn momenteel nog schaars, omdat er nog weinig specialistische cybersecurity-opleidingen zijn. De oplei-

dingsachtergrond is belangrijk, maar niet doorslaggevend. Het gaat er immers om wat iemand kan en wat hij snel kan leren niet hoe hij dat geleerd heeft. Schooluitvallers bevinden zich ook tussen deze professionals. Zij konden in het reguliere onderwijs niet hun draai vinden en hebben zich uit eigen interesse ontwikkeld in cybersecurity.

In de technisch dominante specialistische functies zien we leerroutes via de Informatica en de Techniek. Daarnaast zien we ook hoog gespecialiseerde mensen via aanpalende richtingen binnenstromen zoals uit de natuurwetenschappen en wiskunde. Het eerder gegeven voorbeeld (Hans) laat zien hoe iemand vaak al tijdens een studie de arbeidsmarkt betreedt en daarna weer teruggaat om verder, al dan niet specialistisch, te worden opgeleid. Velen in deze functie betreden de arbeidsmarkt in het bredere veld van informatica en techniek en komen pas later in hun professionele loopbaan op het pad van cybersecurity. Het technisch dominante karakter van de functies vraagt ook later in de loopbaan voortdurende na- en bijscholing en om permanent leren in de werksituatie. Certificaten spelen een grote rol. Deze zijn belangrijk om aantoonbaar bij te blijven in het snel veranderende speelveld.

5.2.1.c Discrepanties op de arbeidsmarkt

In het derde kwartaal van 2014 zijn er voor deze functiegroep ongeveer 40 vacatures gepubliceerd (zie hoofdstuk 3). Op jaarbasis (in 2014) gaat het om ongeveer 150 gepubliceerde vacatures. Op basis van de vacature-analyse en de interviews met werkgevers en CSP's is de verwachting dat er zowel op de korte als middellange termijn kwalitatieve en kwantitatieve discrepanties optreden. Een aantal factoren spelen een rol:

- *Match tussen organisatie en professional:* Organisaties die zoeken naar technisch dominante Cyber Security Professionals weten wie ze zoeken en waar ze moeten zoeken. Er wordt veel via challenges, netwerken of aanbreng-beloningen gewerkt. Echter, voor zeer specialistische functies blijven wervingsmoeilijkheden bestaan. Publieke organisaties hebben meer wervingsproblemen. Zij kunnen niet altijd hetzelfde salaris bieden als het bedrijfsleven. Aan de andere kant kunnen organisaties zoals Politie, Defensie, AIVD een interessant takenpakket neerleggen met aantrekkelijke secundaire arbeidsvoorwaarden. Het blijft desalniettemin een uitdaging om de juiste kwaliteit medewerkers te werven. Consultancy-, detacherings- en adviesbedrijven spelen een aanzienlijke rol in het invullen van gerelateerde taken en functies in organisaties.
- *Standaardiseren van diensten:* Enerzijds wordt verwacht dat een deel van de activiteiten op het vlak van ethical hacking gestandaardiseerd wordt, anderzijds is er een groeiende behoefte aan 'state of the art' kennis op het gebied van dreigingen en de vaardigheden om hier oplossingen voor aan te dragen. Er blijft daarom altijd behoefte aan goede ethical hackers. Zij zijn immers degenen die oplossingen bieden voor de meest geavanceerde hacks. Gestandaardiseerde oplossingen zijn daarbij niet toereikend.
- *Vergroten bewustzijn cybersecurity:* Er is nog een groot aantal organisaties die zich nog onvoldoende bewust zijn van cybersecurity. Daardoor vragen zij (nog) niet om deze specifieke expertise. Het vergroten van het bewustzijn van cybersecurity leidt tot een toename van de vraag naar deze expertise.

Cybersecurityfuncties voor technisch dominante specialisten blijken moeilijk te vervullen. Toch zien we aan de kant van opleidingen dat er veel studenten worden opgeleid in voor cybersecurity-relevante studierichtingen. Als we de private opleidingen buiten beschouwing laten, wordt er een veelvoud van het aantal gevraagde mensen opgeleid. Dat geldt voor cybersecurityfuncties in engere zin en nog sterker als we de analyse verbreden naar cybersecurity relevante vooropleidingen. Tegelijkertijd zien we dat de arbeidsmarkt voor informatici in bredere zin, onderwerp van discussie is. Er lijken dus veel mensen beschikbaar te zijn, echter zij zijn óf niet specifiek met een cybersecurityfocus opgeleid, óf ze zijn onvoldoende gericht op deze functies. Naast de kwantitatieve kant is er natuurlijk ook de kwalitatieve kant, waarbij de kwestie niet alleen is of studenten het juiste vak hebben gestudeerd, maar ook of zij over de gewenste actuele kwaliteit van kennis en

vaardigheden beschikken. De moeilijkheden om de juiste mensen te vinden, hebben mogelijk ook daarmee te maken. Opgeleid zijn voor ICT techniek of security betekent nog niet vanzelf dat er aan de eisen van technisch dominante cybersecurityfuncties wordt voldaan.

5.2.1.d Oplossingsrichtingen

In dit onderzoek komen, wat betreft het voorzien in de behoefte van technisch dominante cybersecurity specialisten, de volgende oplossingsrichtingen naar voren:

Deels kunnen *initiële opleidingen* inspringen in deze behoefte. Zij kunnen enerzijds sterkere cybersecurity-specifieke opleidingen opzetten en anderzijds het aandeel cybersecurity in de huidige opleidingen vergroten. Dit laatste geldt bijvoorbeeld voor informatica-opleidingen. Deze kunnen meer aandacht geven aan dit domein, zodat talentvolle ICT'ers geïnteresseerd raken in een loopbaan in de security.

Het versterken van de cybersecuritycomponent in initiële opleidingen moet wel samengaan met een attitudeverandering van de onderwijsinstellingen. Om effecten te sorteren op de langere termijn is een houding van opleiders vereist die momenteel niet sterk ontwikkeld is (hoog-technisch, niet zuiver theoretisch, maar ook praktijkgericht, werken in een snel-veranderende context, oog hebben voor nieuwe dreigingen en oplossingen, nadruk op creativiteit). In het verlengde hiervan zou het onderwijs en het leren van studenten minder gericht moeten zijn op het ontwikkelen van een 'beheer' mind-set. Het ontwikkelen van een 'gevaren' mind-set moet meer aandacht krijgen. Concreet betekent dit dat het pakket- en modulegericht leren wel onderdeel kan zijn van het curriculum, maar dat studenten daarbij ook moeten worden uitgedaagd om cybersecurity problemen op te sporen en op te lossen waarvoor bestaande programma's en pakketten onvoldoende toereikend zijn.

Van belang is ook dat initiële opleidingen al in een vroeg stadium studenten in contact brengen met bedrijven die laten zien tegen welke cybersecurity-vraagstukken zij aanlopen en welke (interessante) functies daarbij kunnen worden vervuld.

Post-initieel leren is onontbeerlijk. Deze specialisten dienen over 'state of the art' kennis en vaardigheden met betrekking tot cybersecurity (dreigingen en oplossingen) te beschikken. De post-initiële opleidingsmarkt kent een hoge variëteit op dit vlak. Er zijn verschillende opleidingen en cursussen van meer inleidend tot zeer geavanceerd/specialistisch niveau.

Binnen het post-initiële onderwijs kan ook de uitwisseling tussen professionals worden benut om deelnemers een meervoud aan contexten te laten zien en op basis daarvan kennis te ontwikkelen. Voor de toekomst is het van belang dat het post-initieel onderwijs blijft meegroeien met vraagstukken waar professionals in organisaties tegenaan (gaan) lopen. Structureel contact met organisaties in de publieke en private sector is hierbij van belang.

Met betrekking tot de *bedrijfsvoering* kunnen organisaties onder andere door betere arbeidsvoorwaarden hun eigen probleem oplossen. Alleen meer geld bieden zal hierbij niet toereikend zijn. Er zal ook naar de secundaire arbeidsvoorwaarden gekeken moeten worden. Mogelijk worden deze functies dan ook interessanter voor vrouwen. Overigens leiden betere arbeidsvoorwaarden niet rechtstreeks tot een algemene toename van gekwalificeerde professionals. Internationaal werven is een mogelijkheid om op korte termijn tekorten op te vangen. Daarnaast kunnen overheden, bedrijven nadenken over uitwisseling tussen bedrijven en organisaties om kennis en ervaring breder te delen en in te zetten. Publieke organisaties kunnen meer samenwerken en hun professionals regelmatig uitwisselen, om zodoende enerzijds kennis te ontwikkelen en anderzijds de professionals een meervoud aan contexten te laten zien.

Een interessant mogelijk initiatief in dit kader is het opzetten van een 'Young Professional Programme', waarbij jonge professionals binnen een pool van bedrijven voor cybersecurity-taken worden ingezet. Hierbij moet worden opgemerkt dat experts van mening verschillen over de voordelen van deze constructie. Het uitlenen van een professional aan een ander bedrijf heeft nog al eens tot gevolg dat de uitlenende organisatie met een capaciteitsprobleem te maken krijgt. Tegelijkertijd is het de moeite waard om eens nader te onderzoeken waar precies de knelpunten zitten en wat nodig is om de constructie wel goed te laten werken.

Op het vlak van *wervingsmethoden* komt naar voren dat naast de gangbare methoden - o.a. via eigen netwerk, vacatures en d.m.v. het aannemen van (bijna) afgestudeerden na hun stage – andere methoden sterker kunnen worden ingezet, zoals:

- Intern werven: Vooral grotere organisaties kunnen alerter zijn op technische talenten binnen de eigen organisatie en de betreffende professionals een aanbod doen om zich binnen het bedrijf verder te ontwikkelen in een technisch dominante specialistische cybersecurity functie. Dit vraagt uiteraard om een andere mindset van het management binnen organisaties. Managers moeten vanuit het bredere organisatiebelang naar hun personeel kijken en signalen oppikken.
- Aantrekken van zij-instromers: De vijver waaruit gevist kan worden is groter dan men denkt. Organisaties kunnen zich in hun wervingsbeleid richten op aanpalende technische- en ICT functies. Bedrijven moeten aantrekkingskracht ontwikkelen, zichtbaar maken dat zij interessante functies te vervullen hebben waarvoor professionals uit verschillende functies in aanmerking kunnen komen. Dat kan bijvoorbeeld door de interessante kanten van het cybersecuritywerk te benadrukken en het bedrijf zelf kan zich beter als een interessant (ICT) bedrijf neerzetten.

Tot slot kan worden gedacht aan *publieksacties* waarmee op enthousiasmerende wijze aantrekkelijkheid van werk in een technisch dominante cybersecurity functie gepromoot kan worden. Tijdens de bijeenkomst met experts is als voorbeeld het organiseren van 'The Hack of Holland' genoemd.

5.2.2 Niet technisch dominante specialistische functies (functiegroep 2)

Hierbij gaat het om CSP's die meer vanuit een organisatieperspectief naar security kijken. Hierbij onderscheiden we verschillende beroepen en functienamen, zoals IT security officer, IT security specialist, security officer, Information security officer, informatiebeveiliger.

5.2.2.a Kenmerken van de functiegroep

In deze functiegroep gaat het om een professional die zowel het technische perspectief als het organisatieperspectief weet te combineren. Het is typisch een 'schaap-met-vijf-poten professional' die technische kennis en sterke communicatieve vaardigheden combineert. Op de arbeidsmarkt in het algemeen is er een grote vraag naar deze communicatief vaardige doeners. In de vraag (gemeten naar vacatureteksten) lijkt de nadruk op technische vaardigheden en kennis in sommige gevallen overdreven (gezien het minder technische karakter van de functie), maar men moet wel gevoel hebben voor de techniek om met techneuten overweg te kunnen. Deze functionarissen moeten vooral een organisatieperspectief hebben en de organisatie waarin zij werken goed kennen. Zij moeten kunnen schatten wat binnen de organisatorische context belangrijk is. In de meeste gevallen is ruime ervaring vereist, ofwel binnen het bedrijf, ofwel in een soortgelijke functie. Dit is nadrukkelijk geen startersfunctie.

Hieronder is een profiel weergegeven van een typische professional in deze functiegroep.

Lars is 47, heeft zijn opleiding technische informatica 23 jaar geleden afgerond en vond toen een baan als systeembeheerder bij een groot bedrijf in de maakindustrie. Hij heeft alles meegemaakt: nieuwe systemen, migraties en nieuwe toepassingen. Gaandeweg kwam hij erachter dat er niet alleen op functionaliteit gelet moet worden, maar ook op de beveiliging. In eerste instantie ging het om het installeren van firewalls en dergelijke, maar meer en meer ging hij beveiliging als een organisatievraagstuk zien. Binnen het ICT-team kreeg Lars de taak om meer op deze aspecten te letten. Hij volgde trainingen en behaalde een aantal veiligheidscertificaten. Echter, hij voelde zich vaak een roepende in de woestijn.

Dit veranderde 3 jaar geleden toen het bedrijf geconfronteerd werd met een inbraak waarbij de inbrekers gebruik hadden gemaakt van het ICT-netwerk om de toegangspoorten te openen (iets waarop Lars al een tijdje aandacht had proberen te vestigen). Na dit incident is Lars benoemd tot CISO en rapporteert hij direct aan de Raad van Commissarissen. Ook heeft hij een (bescheiden) budget tot zijn beschikking en stuurt hij een aantal mensen aan, die binnen de organisatie een deeltaak op securitygebied hebben.

Echte up-to-date technische ICT-kennis heeft Lars niet, maar hij weet wel welke kennis nodig is om zijn bedrijf veilig te houden. Periodiek huurt hij externen in om penetratietesten uit te voeren.

Hij blijft zich verder ontwikkelen om bij te blijven en wisselt kennis uit met vakgenoten in andere bedrijven en organisaties. De laatste tijd krijgt hij steeds vaker telefoontjes van headhunters of hij toch niet eens wil komen praten. Dat zou toch wel eens interessant kunnen zijn…

5.2.2.b Opleidingsroutes gerelateerd aan deze functiegroep

Het opleidingsprofiel is breed: er is geen specifieke initiële opleiding die leidt tot een functie als security officer. Er is wel een gericht post-intieel aanbod, daarbij gaat het om post-HBO programma's en post-academische master programma's. Deelname daaraan vereist relevante werkervaring. Veel professionals hebben een technische achtergrond en/of een bedrijfskunde-achtergrond. Omdat het vaak gaat om een functie waarin ervaring noodzakelijk is, speelt de precieze initiële opleidingsachtergrond een minder grote rol. Belangrijker zijn ervaring en gevoel voor security issues.

De analyse van de vraag en het aanbod hangt aldus niet louter af van de vraag of er voldoende mensen worden opgeleid voor de gevraagde functies. Veel mensen die in niet technisch dominante functies in de cybersecurity werkzaam zijn, belanden pas wat later in hun loopbaan op dergelijke posities. Eerst wordt ervaring opgedaan, daarna volgen vormen van ervaringsleren, bij- of nascholing en/of weer opnieuw gaan studeren. Daarna worden de functies op het terrein van cybersecurity vervuld, of op een hoger plan gebracht. Van deze groep professionals komen velen uit een breder scala van opleidingen. Veel minder functionarissen hebben opleidingen gevolgd die specifiek op cybersecurity waren gericht. Het gaat daarbij om aanpalende opleidingen in de techniek en informatica, maar ook in veiligheidskunde, juridische opleidingen, bedrijfskunde e.d.

5.2.2.c Discrepanties op de arbeidsmarkt

In het derde kwartaal van 2014 zijn er voor deze functiegroep ongeveer 180 vacatures gepubliceerd (zie hoofdstuk 3). Op jaarbasis (2014) gaat het ongeveer om 600 gepubliceerde vacatures. De verwachting is dat op middellange termijn de vraag naar professionals met dit profiel sterk stijgt. Op de lange termijn echter, zal de vraag stagneren.

Deelklussen waar eerst specialisten voor nodig zijn, zullen organisaties gaandeweg zelf ter hand nemen.

Op basis van de interviews met werkgevers en CSP's blijkt dat er bij dit functieprofiel sprake is van een intransparantie in de arbeidsmarkt. Het aanstellen van een niet technisch dominante cybersecurity specialist is voor veel organisaties de eerste stap om de organisatie cybersecure te maken. Daardoor heeft de organisatie nog niet de kennis om te weten wat zij eigenlijk nodig heeft. Hierdoor ligt de nadruk op technische aspecten en oplossingen. Ook zijn veel kleinere organisaties zich nog onvoldoende bewust dat zij kennis moeten ontwikkelen rond cybersecurity. Wanneer organisaties zich bewust zijn van cybersecurity en het binnen de organisatie hebben opgepakt (door iemand aan te stellen, of extern in te huren), stagneert de vraag naar de professionals (verschuiving van uitbreidingsvraag naar vervangingsvraag).

Het aantal opgeleiden voor deze groep van niet technisch dominante Cybersecurityfuncties is weliswaar opnieuw groot, maar dit leidt niet tot een hoge instroom in Cybersecurityfuncties. Op MBO-, HBO- en WO-niveau worden potentieel meer mensen opgeleid op voor dergelijke functies relevante gebieden dan er vacatures worden aangeboden. Ook hier zien we dus een zeker gebrek aan transparantie. Naast de intransparantie is er op korte en middellange termijn sprake van een kwalitatieve discrepantie. Op zich is het aanbod van professionals die in deze functie kunnen groeien groot (er is geen specifiek opleidingsprofiel), echter kwalitatief zijn veel professionals niet op het gewenste niveau: zij missen of technische kennis, of kennis van de organisatie. Er is een tekort aan professionals met zowel een organisatieperspectief als een technisch perspectief. Het aantal opgeleiden is voldoende, maar de combinatie van technische en organisatiekundige kennis is in de opleidingswereld een uitzondering. Daar ligt wel een behoefte. Ten slotte is er een kwalitatieve discrepantie in de verdere kennisontwikkeling. Deze professionals kunnen binnen hun organisaties nogal eens als eenlingen opereren. Dit kan negatieve gevolgen hebben voor het leren on the job en daarmee voor de verdere kennisontwikkeling binnen organisaties.

5.2.2.d Oplossingsrichtingen

Het aantal potentiële professionals voor niet technisch dominante functies vergroten door meer mensen op te leiden in de initiële opleiding, ligt bij de deze functiegroep niet voor de hand. Met betrekking tot deze functiegroep spelen immers vooral intransparanties en kwalitatieve discrepanties een rol. Bovendien worden bij deze functiegroep professionals met enige jaren ervaring gevraagd (wat nodig is om zowel het technische perspectief als het organisatieperspectief goed te kunnen combineren met gebruikmaking van adequate communicatie) Dit neemt niet weg dat *initiële opleidingen* (bijvoorbeeld Informatica, techniek-studies, bedrijfskunde en economie) aandacht zouden moeten besteden aan cybersecurity vanuit een business continuity perspectief. Zodoende kan de interesse voor cybersecurity worden vergroot waardoor cybersecurity eerder als loopbaanoptie wordt gezien.

Oplossingsrichtingen moeten echter vooral worden gezocht in het post-initiële onderwijs, de bedrijfsvoering en methoden van werven.

In het *post-initiële onderwijs*, is voor mensen die al werken in principe voldoende aanbod aan opleidingen, maar uit de analyse van het opleidingsaanbod van dit type onderwijs blijkt een gebrek aan transparantie. Het is de vraag of professionals en managers (die opleidingsmogelijkheden met hun medewerkers bespreken) hun weg kunnen vinden in dit aanbod. Ook in de interviews met experts kwam de vraag naar voren: welke cursus heb je nodig op welk punt van je loopbaan? En wat kies je als je rekening wilt houden met waar niet alleen nu maar ook in de toekomst behoefte aan is? Nagedacht kan worden over het beter positioneren van opleidingen ten opzichte van elkaar.

Ten aanzien van de *bedrijfsvoering* komen het stimuleren van 'awareness', en imagoverbetering van het werken in dit soort functies naar voren. Bedrijven en organisaties kunnen afzonderlijk en in samenwerking (ook met de overheid) hieraan werken. Ook het uitwisselen van professionals tussen bedrijven en organisaties om het kennisniveau op peil te houden is genoemd. Zowel overheid als bedrijfsleven kunnen nadenken over uitwisseling tussen organisaties om kennis en ervaring breder te delen en verder te ontwikkelen. Hierbij kan bijvoorbeeld gedacht worden aan het organiseren van (werk)conferenties over kwesties waar alle bedrijven en organisaties mee te maken hebben of krijgen. Te denken valt hierbij aan de implicaties van de veranderende datawetgeving (wat betekent dat voor een organisatie en voor de taken van een niet technisch dominante cybersecurity specialist?).

Een in dit onderzoek veel genoemd probleem is dat deze professionals zich vaak eenlingen binnen de organisatie voelen. Organisaties zouden meer kunnen doen om het belang van het CS werk zichtbaar te maken en onder de aandacht van alle medewerker te brengen.

Wat betreft de *werving* geldt net als bij functiegroep 1 dat de vijver waaruit gevist kan worden groter is dan men wellicht denkt. De functie is interessant voor mensen die zich verder in een al ingeslagen weg willen ontwikkelen en nog bij willen leren, maar juist ook voor professionals die toe zijn aan een carrièreswitch. In de werving zou met name dit laatste benadrukt kunnen worden, omdat veel professionals in eerste instantie niet aan de mogelijkheid van een functie waarin ze verschillende soorten kennis en vaardigheden gerelateerd aan cybersecurity kunnen combineren.

In de werving, bijvoorbeeld via vacatureteksten, websites en campagnes zullen de vereiste eigenschappen voor deze functie, anders dan alleen technisch, nadrukkelijker genoemd kunnen worden. Het gaat dan om eigenschappen als kunnen werken in een veranderende dynamische omgeving, samenwerken, communicatieve vaardigheden (in en met alle lagen van de organisatie), empathisch vermogen, regisseren en het managen van veranderingen. In diverse interviews is de verwachting uitgesproken dat juist vrouwen zich beter in een dergelijk profiel zullen herkennen.

Tot slot kan gedacht worden aan het organiseren van 'challenges'. Op kleinere schaal, bijvoorbeeld in onderwijs in samenwerking met het bedrijfsleven gebeurt dit al aan de hand van business cases. Dit zou ook in de vorm van een publieksactie kunnen, waarbij verschillende deskundigen op basis van een scenario een cyberdreiging met mogelijk grote gevolgen voor de organisatie (of breder de regio, de samenleving) moeten oplossen. In de expertgroep werd opgemerkt dat mensen die werkzaam zijn in de cybersecurity een soort jagers mentaliteit hebben, het meedoen aan genoemde challenges zou bij uitstek geschikt zijn om juist die kwaliteiten tot zijn recht te laten komen.

Het steeds verder verhogen van de eisen en het vergroten van de aantallen eisen zal ertoe leiden dat mensen die worden aangenomen in vacante functies omdat ze aan al die eisen voldoen, snel zullen doorgroeien naar hogere functies. Dat kan de continuïteit in het vervullen van de functies in gevaar brengen.

5.2.3 Technisch dominante functies met cybersecurity als onderdeel (functiegroep 3)

Deze beroepen zijn technisch van aard, maar niet gespecialiseerd in cybersecurity. Het betreft een brede groep beroepen waarvoor veelal een cybersecurity-gerelateerd certificaat vereist of een pré is. Voorbeelden zijn: systeembeheerders, softwareontwikkelaars en architects.

5.2.3.a Kenmerken van de functiegroep

De arbeidsmarkt voor deze functiegroep is vergelijkbaar aan de arbeidsmarkt voor ICT'ers in het algemeen. Er is een sterk toenemende vraag. De toename van het gebruik van ICT in een veelheid van toepassingen zorgt ervoor dat bedrijven die traditioneel niet in de ICT-branche werkzaam zijn, nu getalenteerde ICT'ers werven. Veiligheidsaspecten komen meer en meer in de belangstelling te staan. Secure by design wordt voor softwarebedrijven steeds belangrijker.

Anders dan bij de voorgaande functiegroepen gaat het in deze groep wel degelijk om functies waarin starters op de arbeidsmarkt een kans krijgen. Het is zelfs zo dat veel starters al voor het afstuderen een baan aangeboden krijgen (dit geldt voor ICT-afgestudeerden in het algemeen). Een deel van de instroom in deze groep gaat via stages. In veel gevallen wordt het security-deel van de functie binnen het bedrijf zelf opgeleid.

In de vacatureteksten komt naar voren dat certificaten vereist zijn of als pré worden gezien. Er zijn echter ook veel ICT-gerelateerde beroepen waar het veiligheidsaspect nóg minder expliciet is gemaakt: veel ICT'ers zullen zich niet bewust zijn van het feit dat, als zij volgens vastgestelde protocollen programmeren, zij bijdragen aan een meer cybersecure ICT-omgeving. Het gegeven dat cybersecurity meer en meer in reguliere processen zal worden meegenomen, zal zijn weerslag hebben op de vraag (als beschreven in vacatureteksten). Ondanks dat het gebruik van ICT in de toekomst alleen maar zal toenemen en daardoor de nadruk op cybersecurity tevens toeneemt (secure by design), zal de expliciete vraag naar professionals op de arbeidsmarkt op de lange termijn stagneren. Cybersecurity-specifieke taken zullen meer in ieders takenpakket opgenomen worden.

Hieronder is een profiel weergegeven van een typische professional in deze functiegroep.

Hester is 35 jaar en heeft na haar opleiding informatica een aantal banen gehad, voordat zij bij haar huidige werkgever aan de slag kon als programmeur van bedrijfssoftware. Zij werkt er nu vijf jaar.

Sinds twee jaar is er binnen haar bedrijf een CISO aangesteld. Het bedrijf kwam erachter dat de programmatuur vooral gericht was op functionaliteit en minder op veiligheid. Ook gingen klanten steeds vaker vragen stellen rond veiligheidsthema's. De CISO is begonnen om een aantal veranderingen door te voeren zoals jaarlijkse trainingen, awareness raising campagnes en het opstellen van protocollen voor veilig programmeren.

Ook Hester neemt deel aan de trainingen en haar werk is aangepast aan de te volgen protocollen. Ook worden eindproducten voordat ze aan de klant opgeleverd worden, getest door penetratietesters. Dit is af en toe vervelend als er toch nog veiligheidslekken worden gevonden.

Hester zit goed bij haar huidige werkgever en is niet plan van baan te veranderen.

5.2.3.b Opleidingsroutes gerelateerd aan deze functiegroep

Bij deze functiegroep is de relatie tussen de initiële opleiding en de arbeidsmarkt directer. Hierbij moet worden opgemerkt dat er nog niet zo veel brede HBO- en WO opleidingen zijn die cybersecurity in hun programma hebben ingebouwd en er zijn (nog) weinig specialistische cybersecurity-opleidingen. Ontwikkelingen op dit vlak zijn er wel.

De technisch dominant opgeleiden met cybersecurity als onderdeel komen dikwijls direct na hun initiële opleiding de organisaties binnen. Cybersecurity-aspecten gaan vaak pas op den duur een rol spelen in hun werk. Het besef van de noodzaak om meer structureel aandacht te besteden aan cybersecurity-aspecten dringt geleidelijk in de organisaties door. Voor deze groep worden grote aantallen professionals opgeleid. Deze groep wordt Echter, slechts sommigen van hen verschuiven in hun werk vervolgens naar posities waarin cybersecurity in hun takenpakket komt, of krijgen in hun bestaande functies taken op het terrein van cybersecurity. In beide gevallen zien we vervolgens vormen van bij- en nascholing en specialisatie optreden, in samenhang met de ontwikkeling van de vraag naar hun cybersecurity-expertise in hun organisaties. Deze groep wordt dus hoogtechnisch opgeleid, maar wordt pas later in de loopbaan (middels cursussen en certificeringstrajecten) verder in de specialistische taken ingewijd. Omdat cybersecurity voor hen een onderdeel van het werk is, bestaat het risico dat ze in hun werk niet dezelfde ontwikkeling doormaken als de specialistische CSP's. Daarom is na- en bijscholing voor hen extra essentieel.

5.2.3.c Discrepanties op de arbeidsmarkt

In het derde kwartaal van 2014 zijn er voor deze functiegroep ongeveer 70 vacatures gepubliceerd (zie hoofdstuk 3). Op jaarbasis (2014) gaat het om ongeveer 280 gepubliceerde vacatures. Uit de vacature-analyse, literatuurstudie en interviews met werkgevers en CSP's komt naar voren dat de nadruk op security in bedrijven die software ontwikkelen sterk toeneemt. Kwantitatief lijkt er echter geen tekort te zijn aan technisch dominante professionals met security als onderdeel in hun takenpakket. Toch bestaat in de arbeidsmarkt het idee dat er een afstemmingsprobleem bestaat. Dat is waarschijnlijk eerder een kwalitatieve dan een kwantitatieve discrepantie. Wie cybersecurity als deeltaak heeft is meestal al niet CYBERSECURITY-specifiek opgeleid en omdat het niet de enige taak is, ligt snelle kwalitatieve competentieontwikkeling tijdens het werk ook niet voor de hand. Aldus kan er een kwalitatieve discrepantie ontstaan tussen de vraag van de arbeidsmarkt en het specialistische niveau van de gegadigden. Op middellange termijn zal de vraag naar deze professionals daarom stijgen, op lange termijn zal (doordat security meer en meer in het reguliere arbeidsproces wordt opgenomen) de vraag stagneren.

5.2.3.d Oplossingsrichtingen

In principe is vanuit de *initiële opleiding* het huidige opleidingspotentieel voldoende aanwezig om mogelijke tekorten op te lossen. Als er in het algemeen voldoende technici opgeleid worden, er binnen deze opleidingen aandacht is voor cybersecurity en bedrijven zelf willen investeren in het bijbrengen van specifieke securitykennis on the job, zijn tekorten op te lossen.

Met betrekking tot het *post-initiële onderwijs* is het aanbod aan specialistische securitycursussen, aangevuld met interne bedrijfsopleidingen en cursussen, voldoende.

Daarnaast moet ten aanzien van de *bedrijfsvoering* in bredere zin security awareness breder gepropageerd worden binnen de ICT-wereld. Ook kan de overheid eisen stellen ten aanzien van gebruik van protocollen en veiligheidsvoorschriften in softwareontwikkeling waardoor de nadruk op veilige programmatuur toeneemt.

5.2.4 Niet technisch dominante functies met cybersecurity als onderdeel (functiegroep 4)

Hierbij gaat het om functies waarin cybersecurity onderwerp van de kernactiviteit is (bijvoorbeeld jurist in privacy issues, beleidsmedewerker op het gebeid van cybersecurity). Hierbij gaat het dus om juristen, beleidsmakers, auditors e.d. Het gaat steeds om functies waarin cyber eerder als object van een ander domein wordt gezien, dan als kern van de werkzaamheden (bijvoorbeeld als object van beleid of rechtspraak).

5.2.4.a Kenmerken van de functiegroep

Qua carrièreverloop gaat het typisch om mensen die gaandeweg hun loopbaan cybersecurity in hun takenpakket opnemen. Ze hebben een andere achtergrond, wel of geen werkervaring, een interesse in security en ontwikkelen zich verder in de rol die zij binnen hun organisatie krijgen. Deze functiegroep is qua kennisontwikkeling volledig afhankelijk van bijscholing, cursussen en het behalen van certificaten.

Hieronder is een profiel weergegeven van een typische professional in deze functiegroep.

Lodewijk is 37, opgeleid als accountant en werkt voor een accountancykantoor. Dit bedrijf kijkt echter ook naar de ICT-systemen. Door cursussen en het behalen van certificaten (onder andere CISA, CISM) kan Lodewijk sinds 2 jaar als IT-auditor werken. De laatste tijd is er veel werk op dit thema, omdat veel organisaties (zowel publiek als privaat) zich willen laten certificeren (bijvoorbeeld ISO 27001/2).

Hij heeft zich tot senior auditor opgewerkt en stuurt een klein team van collega's aan. Veel van zijn (jonge) collega's hebben een bedrijfskundige achtergrond of zijn, net als Lodewijk, accountant.

5.2.4.b Opleidingsroutes gerelateerd aan deze functiegroep

Voor de niet technisch dominante functies met cybersecurity als onderdeel geldt dat het instroomgebied zo mogelijk nog breder is dan bij alle voorgaande functies. De instroom bestaat uit mensen uit allerlei opleidingen, variërend van administratieve opleidingen en informatie-opleidingen tot veiligheidskundige opleidingen, van financiële opleidingen tot juridische opleidingen. In deze functiegroep zien we mensen die ondanks hun minder technische achtergrond en het feit dat de CYBERSECURITY-taak slechts een onderdeel van hun functie is, moeten kunnen werken in dit zich snel ontwikkelende gebied. Dat vraagt naast initiële opleiding vooral ook om gerichte bij- en nascholing en waar mogelijk leren in de werksituatie. De opleidings- en loopbaanroutes van deze groep tonen de grootste verscheidenheid. Die verscheidenheid creëert nog een extra leernoodzaak om niet alleen op de hoogte te blijven, maar dat ook in samenhang te doen met aanpalende functies en deskundigheden.

5.2.4.c Discrepanties op de arbeidsmarkt

In het derde kwartaal van 2014 zijn er voor deze functiegroep ongeveer 30 vacatures gepubliceerd (zie hoofdstuk 3). Op jaarbasis (2014) gaat het om ongeveer 130 gepubliceerde vacatures. Op basis van de vacature-analyse en interviews met werkgevers en CSP's zijn er voor de nabije toekomst geen indicaties voor grote discrepanties. Er is wel een toenemende vraag, ook op middellange termijn zichtbaar (bijvoorbeeld voor IT-auditors), maar deze functies zijn niet direct gelinkt met één type opleiding. Professionals met een bedrijfskundige achtergrond en een interesse in ICT techniek kunnen in deze functie starten en worden 'on the job' verder bijgeschoold.

Er speelt een algemeen gebrek aan bewustzijn van het belang van cybersecurity onder werknemers (zie paragraaf 5.2.5, overkoepelende discrepanties). Echter, opnieuw moeten we constateren dat er kwantitatief geen probleem kan zijn gezien het grote aantal studenten of deelnemers aan relevante opleidingen. Als er een arbeidsmarktprobleem is, is dat een kwalitatief probleem. Daarin kan een rol spelen dat de actuele kennis ontbreekt, of onvoldoende snel ontwikkeld wordt als cybersecurity slechts een onderdeel van het werk is. Tevens kan het zo zijn dat de diversiteit aan achtergronden een goede match tussen vraag en aanbod van de gewenste expertises bemoeilijkt.

5.2.4.d Oplossingsrichtingen

Het huidige post-initiële opleidingsaanbod is ruim voldoende om te voorzien in de vraag. In de toekomst kan de druk op de post-initiële opleidingen toenemen door een toene-

mende vraag naar dit type professional. Het accent op cybersecurity als deelaspect ligt dikwijls op databescherming/informatiebeveiliging. Regelmatige na-, her-, of bijscholing ten aanzien van zaken als SCADA en de ontwikkelingen in de richting van Internet of things, is daarbij belangrijk. Hoe minder cybersecurity een kerntaak is, hoe groter het risico dat men in de ontwikkelingen op achterstand raakt en daardoor is het belang van actualiseren van de kennis via nascholing des te belangrijker.

5.2.5 Aanpalende functies en overkoepelende discrepanties

Naast directe Cybersecurityfuncties, zijn er aanpalende functies te onderscheiden die indirect de zaak van de cybersecurity dienen. Dergelijke functies bevinden zich in bedrijven, overheden, het onderwijs en in maatschappelijke organisaties. Het gaat onder meer over opleiders die anderen op het belang van cybersecurity wijzen, die onder burgers en gebruikers van ICT het besef van de risico's doen rijzen en die veilig werken helpen bevorderen. Daarnaast gaat het om professionals die in hun sectoren (zoals de gezondheidszorg en het verzekeringswezen) met praktijken te maken hebben waarin cybersecurity een rol speelt. De bedoelde aanpalende functies betreffen functies waarin cybersecurity een rol speelt, zonder dat de betreffende functionarissen zichzelf zullen zien als CSP's (noch in deeltijd, noch anderszins). Ook zullen ze door hun doelgroepen niet als zodanig worden gezien. Toch rust ook bij hen een belangrijke taak om via hun kanalen en mogelijkheden te werken aan cyberveiligheid. Door dat te doen zullen ze vervolgens de aandacht voor cybersecurity en de interesse om zich daarin te scholen of te ontwikkelen kunnen aanwakkeren.

5.2.5.a Opleidingsroute

De leerroutes voor mensen die indirect met cybersecurity te maken hebben verschillen enorm in hun specifieke aandacht voor cybersecurity-gerelateerde vakgebieden en onderwerpen. Er zijn lerarenopleiding met ICT als onderwerp. We zien specifieke minors of vakonderdelen gericht op cybersecurity. Er worden leerroutes bewandeld in medische informatica, Informatica en rechtsgeleerdheid, er zijn vakken gericht op deelterreinen zoals privacy of social media. Het relatieve belang van de cybersecurity-invalshoek is in die leerroutes vaak niet groot. Het relatieve belang van deze functies en functionarissen is echter groot als het gaat om het bevorderen van cybersecurity awareness en naleving van gedragsregels.

5.2.5.b Discrepanties

De arbeidsmarkt is op dit punt nog in een pril stadium van ontwikkeling. Veel mensen die op deze indirecte wijze met cybersecurity te maken hebben, worden niet op hun kwaliteiten ten aanzien van cybersecurity geworven of geselecteerd. Toch ligt juist bij hen vaak de taak om leerlingen, cliënten, patiënten, relaties of collega's te doordringen van cyberrisico's en mogelijkheden te bieden die te omzeilen.

Het aantal beschikbare afgestudeerden of opgeleiden is wederom ruim. De cybersecurity-aspecten van de functies blijven in werving en selectie vaak een nevenaspect.

In het voorgaande is al een paar keer aangestipt, dat naast de arbeidsmarktdiscrepanties er ook een belangrijke algemene discrepantie bestaat die invloed heeft op de arbeidsmarkt. Hierbij gaat het om een algemeen tekort aan kennis en bewustzijn voor security. Dit gebrek veroorzaakt enerzijds dat organisaties en (met name kleine) bedrijven de gevaren van cyber voor hun organisaties onderschatten. Anderzijds zijn jongeren zich onvoldoende bewust van de loopbaanmogelijkheden binnen cybersecurity.

5.2.5.c Oplossingsrichtingen

Het oplossen van genoemde bredere discrepanties vereist een breder perspectief dan hiervoor gehanteerd. Bedrijven moeten zich meer bewust worden van de noodzaak om cybersecurity serieus te nemen. Een eerste stap is iemand aanstellen die vanuit een organisatieperspectief naar veiligheidsaspecten kijkt. Nagedacht kan worden om, in navol-

ging van de 'stop cybercrime scan'[104], maatwerk advies aan te bieden en bedrijven/organisaties te assisteren in het opstellen van functieprofielen (wat heeft een organisatie eigenlijk écht nodig?). Ook moeten organisaties kennisuitwisseling organiseren om het kennisniveau op peil te houden. Cybersecurity is niet iets waar bedrijven op moeten concurreren (banken doen dit nu al). Veiligheid is een gezamenlijke verantwoordelijkheid en vraagt om uitwisseling van kennis en ervaring. Daarnaast moet een breder en beter bewustzijn gecreëerd worden voor cybersecurity in het onderwijs, op social media en daar waar mensen en in het bijzonder jongeren komen. Hierin ligt een gezamenlijke verantwoordelijkheid voor bedrijfsleven, overheid, onderwijs en de burger.

[104] https://scans.mkbservicedesk.nl/stopcybercrime

6 Conclusies

De hoofdvragen in dit onderzoek zijn:

1) In hoeverre is er, nu en in de toekomst, een mogelijk kwalitatief en kwantitatief tekort aan Cyber Security Professionals (CSP's) op hoger en middelbaar niveau te verwachten?
2) Hoe kunnen eventueel geconstateerde tekorten op de huidige en toekomstige arbeidsmarkt voor Cyber Security Professionals worden opgelost?

Om antwoord te geven op deze vragen richtte het onderzoek zich op de volgende aspecten (zie hoofdstuk 1, paragraaf 1.4):

A. Kenmerken van cybersecurity en CSP's.
B. Invloed van omgevingsfactoren op de arbeidsmarkt van CSP's.
C. De vraag naar CSP's op de arbeidsmarkt.
D. Het aanbod vanuit onderwijs en opleidingen op het terrein van cybersecurity.
E. Discrepanties tussen vraag en aanbod op de arbeidsmarkt.
F. Oplossingsrichtingen voor de gevonden discrepanties op de korte en middellange termijn.

De hieronder geformuleerde conclusies zijn gerelateerd aan deze aspecten. Dit mondt (aan het eind van dit hoofdstuk) uit in de integrale beantwoording van de twee hoofdvragen van dit onderzoek.

6.1 Conclusies

In de literatuur wordt het begrip en domein cybersecurity niet eenduidig en nog te veel vanuit het ICT perspectief beschreven. Werken aan veilige ICT-omgevingen heeft tot doel kernprocessen van organisaties veilig te laten verlopen en cybersecurity refereert aan de kwetsbaarheid van bedrijven, burgers, overheid en de maatschappij als geheel. Aan deze kwetsbaarheden en het oplossen daarvan, zitten zowel technische ICT-aspecten als interactie (mens-ICT) aspecten. Hierin zijn verschillende rollen en taken te vervullen. Dit maakt cybersecurity niet alleen een technisch ICT-vraagstuk, maar vooral ook een organisatievraagstuk.

Conclusies 1: Cybersecurity is zowel een ICT- als een organisatievraagstuk. Cybersecurity moet vooral ook bekeken worden vanuit een breder organisatieperspectief waarin verschillende rollen en taken te vervullen zijn.

Het werkveld van de CSP's is sterk onderhevig aan veranderingen. De snel veranderende digitale wereld met daarbij komende dreigingen en noodzakelijke veiligheidscriteria stelt hoge eisen aan publieke en private organisaties om cybersecure te zijn of te worden. Zowel de frequentie van incidenten, als de impact daarvan, in termen van directe schade en indirecte schade (bijvoorbeeld imago schade), neemt toe. Bedrijven en publieke organisaties worden zich meer en meer bewust van het feit dat cybersecurity niet alleen een ICT-issue is, maar een integraal thema. Cybersecurity is van een ICT-vraagstuk een 'boardroom issue' geworden, want het voortbestaan van het bedrijf kan in het geding komen. Toenemende beleidsaandacht voor cybersecurity, de noodzaak van het zich bewust zijn van de risico's (aangezien internet zich op alle terreinen van het dagelijkse leven manifesteert) en veranderingen in wetgeving (op het gebied van privacy en data protectie) hebben een extra stuwend effect op de vraagontwikkeling.

Conclusie 2: Twee factoren houden het werkveld van de Cyber Security Professional sterk in beweging. Enerzijds gaat het hierbij om maatschappelijke ontwikkelingen (op politiek, economisch, sociaal, technisch en juridisch terrein). Anderzijds vragen incidenten (afhankelijk van frequentie en impact) om aanpassingen in het werkveld.

In de literatuur komen drie dimensies naar voren waarmee functies van Cyber Security Professionals kunnen worden beschreven:

- Werkzaamheden kunnen als *technisch dominant* of als *niet technisch dominant* worden getypeerd. Technisch dominant wil zeggen dat de nadruk ligt op het ICT-perspectief. Bij niet technisch dominante functies staat het organisatieperspectief meer centraal.
- De functie kan *specifiek op cybersecurity gericht* zijn of *cybersecurity als onderdeel* hebben.
- De functie kan *operationeel-tactisch* of *tactisch-strategisch* georiënteerd zijn.

Op basis van deze dimensies en bestudering van vacatureteksten kunnen vier groepen van functies worden onderscheiden:

1) *Technisch dominante specialistische cybersecurityfuncties*. Deze functies zijn zeer specifiek op IT/informatiebeveiliging gericht en hebben een grote technische component. Voorbeelden van functies zijn: ethical hackers, penetratietesters, software testers en technical security-engineers.
2) *Niet technisch dominante specialistische cybersecurityfuncties.* Hierbij gaat het om cybersecurityspecialisten die meer vanuit een organisatieperspectief naar security kijken. Voorbeelden van functies zijn: IT security officers, IT security specialists, security officers, Information security officers, informatiebeveiligers.
3) *Technisch dominante functies waarbij cybersecurity een onderdeel is*. Deze beroepen zijn technisch van aard, maar niet gespecialiseerd in cybersecurity. Het betreft een brede groep beroepen waarvoor veelal een cybersecurity-gerelateerd certificaat vereist is of als pré wordt aangemerkt. Voorbeelden van functies zijn: systeembeheerders, softwareontwikkelaars en architects.
4) *Niet technisch dominante functies waarbij cybersecurity een onderdeel is.* Dit is de minst afgebakende functiegroep. Hierin bevinden zich tal van functies zoals beleidsmedewerkers, juristen, directeuren, auditors. Bij deze functies kan cybersecurity onderwerp van de kernactiviteit zijn (bijvoorbeeld jurist in privacy-issues, beleidsmedewerker op het gebied van cybersecurity). Daarnaast gaat het om functies waarin cyber eerder als object van een ander domein wordt gezien (bijvoorbeeld object van beleid, rechtspraak) dan als kern van de werkzaamheden.

Het onderscheid operationeel-tactisch en tactisch-strategisch komt in alle vier de functiegroepen terug

Conclusie 3: Op basis van de literatuur en bestudering van vacatureteksten, worden voor de Cyber Security Professional vier functieprofielen onderscheiden die in het kader van arbeidsmarktonderzoek gebruikt kunnen worden:

- *technisch dominante specialistische cybersecurityfuncties*;
- *niet technisch dominante specialistische cybersecurityfuncties;*
- *technisch dominante functies waarbij cybersecurity een onderdeel is;*
- *niet technisch dominante functies waarbij cybersecurity een onderdeel is.*

Wat betreft de vraag naar CSP's op de arbeidsmarkt en de totale werkgelegenheid voor CSP: In de eerste drie kwartalen van 2014 zijn 916 vacatures gepubliceerd met betrekking tot het cybersecuritydomein. Op jaarbasis (gerekend over het laatste kwartaal van 2013 en de eerste drie kwartalen van 2014) gaat het om ongeveer 1.158 gepubliceerde vacatures. De totale vraag zal groter zijn, omdat informele wervingskanalen en challenges[105] gericht op werving niet als vacatures tellen in de vacature-analyse.

Om een indruk te krijgen van de totale werkgelegenheid (het totaal aantal arbeidsplaatsen) in het cybersecuritydomein, maken we een vergelijking met de aantallen gepubliceerde vacatures en de werkgelegenheid in de brede ICT-sector. In de brede ICT-sector staat één vacature tot zes arbeidsplaatsen.[106] Passen we deze zelfde verhouding tussen vacatures en arbeidsplaatsen toe op het cybersecuritydomein, dan wordt op basis hiervan de totale werkgelegenheid binnen dit domein geschat op 7.000 arbeidsplaatsen.

Op basis van de omgevingsanalyse (het maatschappelijk belang en de rol van incidenten nemen toe, zie conclusie 2) wordt verwacht dat de vraag naar Cyber CSP's zal stijgen. Enerzijds neemt de urgentie van het inzetten van kennis en kunde op dit terrein toe. Anderzijds wordt het cybersecuritydomein steeds meer ook als een organisatievraagstuk gezien en an sich breder opgevat (multidisciplinair).

De verwachte stijging van de vraag geldt voor alle vier de functiegroepen en ook voor aanpalende functies. Ten aanzien van deze stijging geldt dat de vraag naar MBO-opgeleiden binnen de ICT zal afnemen (door digitalisering en automatisering van werkzaamheden). De vraag naar hoger opgeleiden daarentegen zal toenemen.

Conclusie 4: Weliswaar is het aantal zichtbare vacatures momenteel nog bescheiden, echter er zijn indicaties (toename van de urgentie en bredere opvatting van het cybersecuritydomein) dat de vraag naar CSP's (in zijn totaliteit) in de toekomst zal toenemen. Dat geldt vooral voor hoger opgeleiden en in mindere mate voor op MBO-niveau opgeleide professionals.

De vraag zal dus over de gehele linie stijgen. Daarbij is sprake van accenten per functiegroep:

1) *Technisch dominante specialistische cybersecurityfuncties.* De arbeidsmarkt voor dit profiel wordt, naast grote werkgevers (zowel banken, politie en defensie) gedomineerd door consultancybedrijven. Deze specialisten (hackers, pentesters) delen met cybercriminelen de rol van 'front-runner' in de ontwikkeling van cybersecurity. Om de verdere technologische ontwikkeling van cybercrime bij te benen, zal de vraag naar deze specialisten aanhoudend stijgen.
2) *Niet technisch dominante specialistische cybersecurityfuncties.* De arbeidsmarkt voor dit functieprofiel kent een gedifferentieerder palet aan vragende organisaties. Het aanstellen van dit type CSP is voor veel organisaties de eerste stap in het op orde brengen van de cybersecurity. In veel gevallen is één CSP voldoende om de security te organiseren. Specialistische taken worden via inhuur van derden uitgevoerd. Na een sterke groei in de eerste vijf jaar zal de vraag naar niet technische dominante cybersecurityfuncties licht dalen, doordat organisaties hun beveiliging in de organisaties hebben ingebed. Tegen die tijd zal echter de vervangingsvraag ook een rol gaan spelen in de ontwikkeling van de vraag. Professionals met erva-

[105] Een 'challenge' wordt in dit onderzoek omschreven als een uitdagende wervingsactiviteit met een *gaming* karakter, waarbij vraagstukken op het terrein van cybersecurity moeten worden opgelost.

[106] In 2013 was de totale werkgelegenheid in de ICT/automatisering ongeveer 300.000 (zie tabel 1; bron: Panteia op basis van P-Direkt en Enquête beroepsbevolking, CBS). Het totaal aantal vacatures op jaarbasis is ongeveer 50.000 (zie figuur 4; bron: Panteia/PLATO op basis van vacatureanalyse Jobfeed). De verhouding tussen het aantal vacatures en de totale werkgelegenheid is daarom 1 : 6.

ring in het cybersecuritydomein gaan met pensioen. In vacatures zal met betrekking tot deze groep functies vaker om ervaren mensen worden gevraagd.

3) *Technisch dominante functies waarbij cybersecurity een onderdeel is.* In de arbeidsmarkt voor dit functieprofiel wordt de grootste groei verwacht. Deze markt wordt bepaald door software-ontwikkelaars. Deze bedrijven zijn zich de laatste jaren gaan toeleggen op verbeterde beveiliging van hun software (secure by design) en vragen ICT'ers met security-ervaring, -certificaten of -affiniteit. Aangezien meer en meer organisaties als softwarebedrijven gezien kunnen worden (ICT is de kern van veel bedrijven), neemt de vraag naar deze technici in de toekomst toe. De vraag naar veiligere systemen weerklinkt in de systeemontwikkeling en systeembeheersing.
4) *Niet technisch dominante functies waarbij cybersecurity een onderdeel is.* De arbeidsmarkt voor dit functieprofiel kent een veelheid aan verschillende functies, waarbij sommige professionals niet eens beseffen dat zij zich bezighouden met cybersecurity. In de toekomst zullen vaker en nadrukkelijker competenties ten aanzien van cybersecurity-gerelateerde taken worden gevraagd.

Conclusie 5: Een stijging van de vraag geldt voor alle functiegroepen, maar de grootste groei wordt verwacht bij de technisch dominante functies waarbij cybersecurity een onderdeel is.

Wat betreft onderwijs en opleiding op het terrein van cybersecurity, komt een een rijk en divers aanbod naar voren. Er bestaan veel aanbiedingsvormen naast elkaar, zoals initiële opleidingen, post-initieel onderwijs, korte cursussen, masterclasses, workshops, seminars, on the job leren, afstandsonderwijs, en in-company training.
De opleidingen worden op talrijke locaties aangeboden. Er zijn initiële en post-initiële opleidingen van MBO- tot WO-niveau. Ook in de private sector is het aanbod groot. Hierbij ligt een accent op het up-to-date houden van kennis en vaardigheden van werkenden.

Ook voor wat betreft inhoud en diepgang is de range van het aanbod breed. Deze bestrijkt opleidingen met duidelijke technische en informatica-inhouden én opleidingen met duidelijke veiligheids-, juridische, of forensische inhouden. Ook zijn er opleidingen die deelnemers indirect, maar diepgaand scholen in voor cybersecurity relevante vakken en competenties. In die categorie vallen opleidingen die een sterke ICT-component hebben maar gericht zijn op andere dan technische- of veiligheidsgebieden, zoals kunstmatige intelligentie, studies methoden en technieken, medische informatiekunde, logistiek, meet- en regeltechniek, etc. Al met al is er een veel breder aantal opleidingen dat aan de kennis en kunde van studenten/deelnemers bijdraagt, dan alleen de direct op ICT-, of internet- en cybersecurity gerichte opleidingen.

De veelheid aan opleidingen, cursussen en aanbiedingsvormen leidt echter ook tot intransparantie van het aanbod. Informatie over onderwijs- en opleidingstrajecten is op zich wel te achterhalen, maar wat ontbreekt is één helder overzicht van de opleidingsmogelijkheden en -routes in relatie tot de competenties waarvoor deelnemers willen en/of moeten worden opgeleid.

Conclusie 6: Het opleidingsaanbod gerelateerd aan cybersecurity is divers en omvangrijk. Opleidingen worden vaak op verschillende locaties aangeboden en er is veel variatie in aanbiedingsvormen. Tegelijkertijd is het aanbod weinig transparant.

Wat betreft het kwantitatieve aanbod van CSP's vanuit onderwijs en opleidingen, is er een groot potentieel aan professionals die in principe inzetbaar lijken. In 2014 blijken er ruim voldoende deelnemers in een relevante vooropleiding te zitten:

- een instroom van 6.880 deelnemers op MBO 4 niveau;
- een instroom van 73 deelnemers op HBO associate degree niveau;
- een instroom van 4.053 deelnemers op HBO niveau;
- een instroom van 292 deelnemers op Master niveau;
- een instroom van deelnemers aan post-academische of post-executive masters van (zoals blijkt uit de interviews) zeker 200 personen.

Zelfs als we rekening houden met een uitval van 50%, blijven de aantallen nog hoog in vergelijking met de beschikbare vacatures. Tegelijkertijd leiden deze aantallen maar zeer beperkt tot instroom in cybersecurity-gerelateerde functies. MBO'ers vervolgen hun opleiding vaak op HBO-niveau. Veel bredere HBO- en WO-opleidingen hebben cybersecurity maar beperkt in het programma ingebouwd en er zijn (nog) weinig specialistische cybersecurityopleidingen. Dit leidt ertoe dat studenten niet of pas relatief laat cybersecurity als optie meenemen in hun overwegingen ten aanzien van hun verdere studie of loopbaan.

Conclusie 7: Het opleidingspotentieel is in principe toereikend om te voorzien in de vraag naar CSP's. Het is echter de vraag of deelnemers aan cybersecurity-gerelateerde opleidingen cybersecurity als loopbaanoptie zien.

Er wordt dus een toename van de vraag naar CSP's verwacht en het potentieel aan professionals is in principe voldoende. Tegelijkertijd moet echter (op basis van interviews met deskundigen uit 24 publieke- en private organisaties) worden geconstateerd dat functies moeilijk te vervullen zijn. Oorzaken hiervoor blijken gerelateerd aan kwalitatieve discrepanties en intransparanties op de arbeidsmarkt.
De opgave lijkt niet zozeer te zijn om meer mensen op te leiden, maar veeleer om hen tijdens hun opleiding te interesseren voor cybersecurity en voor banen in die sector. Samengevat komen de volgende discrepanties naar voren:

- Studenten worden weliswaar opgeleid in voor cybersecurity relevante studierichtingen, maar zij missen een specifieke gerichtheid op cybersecurity.
- Veel organisaties hebben onvoldoende kennis over wat zij eigenlijk nodig hebben, wie ze precies zoeken en waar ze die kunnen vinden.
- Er is voldoende aanbod, maar de professionals hebben nog niet het gewenste niveau: zij missen (afhankelijk van de functie en de taken) òf technische kennis òf kennis van de organisatie.
- Professionals hebben cybersecurity als deeltaak erbij gekregen, maar zijn niet specifiek opgeleid op dat terrein. Omdat zij veel andere taken hebben ligt snelle kwalitatieve competentie-ontwikkeling op het terrein van cybersecurity ook niet altijd voor de hand.

Conclusie 8: In kwantitatieve zin hoeft er geen sprake te zijn van tekorten. De aansluiting van de vraag naar CSP's en het aanbod van deze professionals wordt gehinderd door intransparanties en kwalitatieve discrepanties.

Met het oog op het duurzaam oplossen van discrepanties op de arbeidsmarkt, komen (mede benadrukt door in het onderzoek betrokken experts op het terrein van cybersecurity) de volgende oplossingsrichtingen naar voren:

1. De mogelijkheden van het onderwijs benutten bij het oplossen van discrepanties.
Het gaat hierbij om het bevorderen van bewustzijn onder leerlingen en studenten in het algemeen, het motiveren tot voor cybersecurity relevante studiekeuzes bij een deel van de leerlingen en studenten en het gericht, zelfs specialistisch, opleiden van een nog specifiekere groep. Leren en professionaliseren in een zich snel ontwikkelend veld als de cybersecurity vereist bij uitstek een vorm van een leven lang leren. In het kader van een

leven lang leren is het van belang, ook te zoeken naar efficiënte en effectieve manieren om in werksituaties de kennis verder te ontwikkelen, te delen en te vertalen in verbeteringen en innovaties. De werkomgeving strekt verder dan alleen de eigen organisatie.

Behalve professionalisering in de zin van persoonlijke ontwikkeling in het beroep, is er ook de noodzaak van ontwikkeling van het vak. Cybersecurity is een terrein waar op verschillende niveaus, veel werk wordt verricht in allerlei publieke en private organisaties (van klein tot groot) en industrieën. Ook de opleidingswereld draagt bij aan de ontwikkelingen in het cybersecuritydomein. Samenwerking van alle betrokken partijen is van vitaal belang voor het 'up to date' blijven van de cybersecuritysector en allen die daarin werkzaam zijn. We zien dit vertaald in actieve betrokkenheid van ICT-bedrijven in opleidingen, in deelname van practici als docenten in hogere opleidingen, en in participatie van wetenschappers in het oplossen van praktische problemen.

2. *Veranderen van werkprocessen in organisaties en samenwerking tussen organisaties, om zodoende het niveau van cybersecurity op peil te brengen en te houden.*

In het onderzoek komen op dit vlak de volgende mogelijkheden naar voren:

- gelegenheid creëren binnen en tussen organisaties om kennis te delen en van elkaar te leren;
- verbeteren van secundaire arbeidsvoorwaarden, wat het werk voor meer groepen zoals vrouwen, extra aantrekkelijk kan maken;
- efficiënter en gerichter werven (ook binnen de eigen organisatie, door functionarissen opmerkzaam te maken op de mogelijkheden om door te groeien in een aan cybersecurity gerelateerde functie);
- inzet van een pool van professionals vanuit verschillende organisaties, outsourcing en inhuren van externe specialisten;
- zichtbaar maken van het werk van de CSP binnen de organisatie en het nut daarvan;
- hanteren van een minder hiërarchische organisatiestructuur (geldt voor grotere organisaties).

3. *Verhelderen van onderwijs- en opleidingsroutes.*

De relatie tussen opleidingstrajecten en –routes, te verwerven competenties, uit te oefenen functies en te bereiken posities op de arbeidsmarkt is diffuus. De trajecten die loopbaanontwikkeling in de cybersecurity ondersteunen zijn dat ook. Keuzes maken in het woud van mogelijkheden is niet altijd eenvoudig. Daar ondervinden zowel de mensen die het aangaat als de organisaties de nadelen van. Het betekent dat te vaak de juiste man of vrouw op de verkeerde plek belandt. Het leidt tot inefficiënte en ineffectieve leer- en loopbaanroutes. Het verhelderen van de onderwijs- en opleidingstrajecten en –routes, zal een positieve uitwerking hebben op de kwaliteit van het aanbod en de toeleiding van uitstromende deelnemers en studenten naar functies op het terrein van cybersecurity.
Deze oplossingsrichting verwijst ook naar een leven lang leren. Het werkveld van cybersecurity vraagt om permanente actualisering van kennis en het 'up to date' houden van vaardigheden. In dat kader groeit de noodzaak om gestalte te geven aan een systeem van onderhoud van kennis, actualisering van kennis en kennisontwikkeling.

4. *Monitoren van ontwikkelingen in de samenleving, het onderwijs en opleidingen en arbeidsmarkt. De hierdoor verkregen gegevens kunnen de aansluiting van de vraag naar en het aanbod van CSP's op de korte en (middel)lange termijn ten goede komen.*

In het verlengde van oplossingsrichting 3 kan dataverzameling en registratie over opleidingen en de vraag op de arbeidsmarkt een bruikbaar middel voor kwaliteitsverbetering zijn. Het onderzoek naar de arbeidsmarkt voor Cyber Security Professionals, zoals beschreven in dit rapport, biedt een stand van zaken. De samenleving in zijn totaliteit en het werkgebied van de CSP's zijn sterk in beweging. Een vorm van monitoring van ontwikkelingen in de samenleving, de arbeidsmarkt en de opleidingsmarkt kan de aanslui-

ting van de vraag naar en het aanbod van CSP's op de kortere en langere termijn ten goede komen.

5. *Het imago van het cybersecuritywerkveld en de -functies sterker en uitdagender neerzetten.*

Cybersecurityfuncties worden nog al eens geassocieerd met een bepaald soort ethical hacker die volledig opgaat in zijn vak (met zwart T-shirt, paardenstaart etc.). Aan de andere kant worden cybersecurityfuncties in verband gebracht met 'moeilijkdoeners binnen de organisatie': immers door hun oriëntatie op alles wat er mis kan gaan, zijn zij in de ogen van anderen wel een beetje moeilijk. De uitdagende, vooruitstrevende, en complexe aspecten van het werk mogen meer op de voorgrond worden gebracht. Een andere kwestie is dat de sector vooral uit mannen bestaat. Op het terrein van cybersecurity zijn verschillende functies te vervullen waarbij verschillende soorten competenties vereist zijn. Dat maakt het werkveld interessant voor mannen en vrouwen. Een positieve uitstraling van de mogelijkheden en uitdagingen maakt de vijver waaruit kan worden gevist groter. Voorlichting, scholing en eventueel publieksacties (bijvoorbeeld in de vorm van challenges) kunnen ook bijdragen aan verandering.

6. *Cybersecurity oppakken als een gezamenlijke verantwoordelijkheid van burgers, overheid, organisaties en onderwijs: gericht op bewustwording.*

Alle geraadpleegde organisaties en deskundigen zijn het erover eens: cybersecurity is een kwestie die het leven van vrijwel iedere burger beïnvloedt. Daarom is het belangrijk om gericht op de hele samenleving, te werken aan bewustwording. Het doel hiervan is dat iedereen zich bewust wordt van de risico's en de mogelijkheden zich daartegen te weer te stellen. Er ontstaat aldus een behoefte om deskundigen op te leiden en in te zetten, die die bredere groep van burgers weten te bereiken met de boodschap dat cybersecurity vraagt om alertheid, maatregelen en controles op het gebied van informatieveiligheid.
Dit houdt ook in dat cybersecurity meer gezien moet worden als iets wat altijd en overal een rol speelt waar mensen met ICT-systemen werken en interacteren. Hierin ligt ook een taak voor het funderend onderwijs (primair en secundair onderwijs). Hoe daaraan vorm te geven, zal in toekomstig onderzoek verder moeten worden uitgezocht.

Conclusie 9: Oplossingsrichtingen voor discrepanties op de arbeidsmarkt voor CSP's hebben betrekking op:

1) *Benutten van de mogelijkheden van onderwijs en opleidingen op het vlak van (o.a.) bewustwording, studiekeuze, verduidelijken van opleidingsroutes en mogelijkheden voor een leven lang leren op het terrein van cybersecurity.*
2) *Versterken en verbeteren van werkprocessen in organisaties en bevorderen van samenwerking tussen organisaties.*
3) *Verhelderen van onderwijs- en opleidingsroutes.*
4) *Monitoren van ontwikkelingen in relatie tot de arbeidsmarkt van CSP's.*
5) *Verbeteren en versterken van het imago van het cybersecuritywerkveld en de CSP.*
6) *Doorgaan op de ingeslagen weg om cybersecurity te benaderen als een gezamenlijke verantwoordelijkheid van burgers, overheid, organisaties, onderwijs en opleidingen: gericht op bewustwording.*

6.2 Slotconclusie

Hoofdvraag 1 van dit onderzoek luidt: *In hoeverre is er, nu en in de toekomst, een mogelijk kwalitatief en kwantitatief tekort aan Cyber Security Professionals (CSP's) op hoger en middelbaar niveau te verwachten?*

Het antwoord op deze vraag is, dat de vraag naar CSP de komende vijf jaar als gevolg van vele veranderingen en ontwikkelingen gerelateerd aan het cybersecuritydomein zal stijgen. Het potentieel aan CSP's is in principe voldoende om aan de vraag te blijven voldoen. Er worden voldoende professionals opgeleid. Er wordt dus geen kwantitatief tekort verwacht. Daarentegen spelen er momenteel en zullen er op de korte termijn aansluitingsproblemen spelen. Vraag en aanbod kunnen elkaar niet zo goed vinden. Vooruitlopend op de tweede hoofdvraag van dit onderzoek lijkt de opgave niet zozeer te zijn om meer mensen op te leiden, maar veeleer om hen tijdens hun opleiding en in hun werk te interesseren voor cybersecurity en voor functies in die sector.

Hoofdvraag 2 van dit onderzoek betreft: *Hoe kunnen eventueel geconstateerde tekorten op de huidige en toekomstige arbeidsmarkt voor Cyber Security Professionals worden opgelost?*
In dit onderzoek zijn niet zo zeer tekorten als wel kwalitatieve discrepanties en intransparanties op de arbeidsmarkt voor CSP's geconstateerd. Hiervoor zijn in dit onderzoek diverse oplossingsrichtingen voorgesteld waarvan de voornaamste betrekking hebben op: kennis delen en bundelen; vergroten van transparantie in het opleidingsaanbod, versterken van het imago van het beroep; en werken aan bewustwording in alle sectoren van de samenleving.
Oplossingen op deze terreinen kunnen bijdragen aan een duurzame en goede balans van de vraag naar en het aanbod van CSP's op de arbeidsmarkt.

Bijlage 1: Literatuuroverzicht

Advies CSR dd 31-07-2013 : https://www.ncsc.nl/organisatie/samenwerkingspartners/publiek-privaat/csr.html.

Anderson, R. (2001), "Why information security is hard − an economic perspective", ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference, IEEE Computer Society, Washington, DC.

Anderson, R., et al., 2012. Measuring the cost of cybercrime. Workshop on the Economics of Information Security (WEIS) [online]. Available from: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf [Accessed 10 December 2012].

Baltimore Cyber Technology & Innovation Center (CTIC), (2013), Cyber Security Jobs Report.

Bernaards, F e.a., High Tech Crime, Criminaliteitsbeeldanalyse 2012, Driebergen 2012.

Boer, L.J.M. & A.R. Lodder (2012), Chapter 10 Cyberwar (Cyberwar: What Law to Apply? And to Whom?), in: Leukfeldt/Stol (eds.), Cyber Safety: An Introduction, Eleven Publishing, zie ook http://ssrn.com/id=2039220

Bos, H, "We hebben hackers nodig" in: Magazine Nationale veiligheid en crisisbeheersing, jaargang 11, nummer 6 december Den Haag 2013.

Bouman, A., Varkenscycli op de arbeidsmarkt, Economisch Statistische Berichten, 23 augustus 1989.

Breugel van G. en Córvers F., Arbeidspotentieel voor de politie, nu en in de toekomst, Maastricht 2010.

Bronk, C. and A. Pridgen (2013). Cybersecurity Issues and Policy Options for the U.S. Energy Industry. Baker Institute Policy Report, No. 53, September 2012. Rice University - Department of Computer Science.

Burning Glass (2014), Job Market Intelligence: Report on the Growth of Cybersecurity Jobs

Burley, D. L. (2014), Department of Human and Organizational Learning, George Washington University, Ashburn, Virginia, USA. Cybersecurity education, part 1. In: ACM Inroads.

Burley, D.L., Jon Eisenberg, and Seymour E. Goodman (2014). Would cybersecurity professionalization help address the cybersecurity crisis?: Evaluating the trade-offs involved in cybersecurity professionalization. In: Communications of the acm, Vol. 57, no. 2 Homeland Security Advisory Council. Cyber Skills Task Force Report. Department of Homeland Security, Washington, D.C., 2012.

Burton, Joe (2013), Small states and cyber security, in: Political Science, 2013, Vol.65(2), pp.216-238 [Peer Reviewed Journal].

Cap Gemini, Meer vissen in de vijver met de White hat Office, Den Haag 2013.

Cap Gemini, Trends in Veiligheid 2013, Een digitale samenleving kan niet zonder digitale veiligheid, Utrecht 2013 p. 62-66.

CEN Workshop on ICT Skills (2014). European e-Competence Framework 3.0. Retrieved from: http://profiletool.ecompetences.eu. Er is ook een Nederlandse versie 2.0 (uit 2010) van dit framework beschikbaar: Europees e-Competence Framework 2.0: http://www.ecompetences.eu/site/objects/download/5228_eCFversie162341NPRCWA2010def.pdf

Center for Strategic and International Studies (2014), Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II.

Chang, J. Morris (2013). New Trends in Cybersecurity. In: IT Professional, Vol. 15, No. 4, pp. 2-3. Published by the IEEE Computer Society.

Clark, R.A. & R.K. Knake (2010), Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins. Feiler, L. (2012), Information Security Law in the EU and the U.S. A Risk-Based Assessment of Regulatory Policies, Springer.

Conklin, W.A., Cline, R.E., Roosa, T; Univ. of Houston, Houston, Texas, USA (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors.

In: System Sciences (HICSS), 2014 47th Hawaii International Conference on System Sciences.
Curtis, Scipiaruth Kendall (2012). Commitment to Cybersecurity and Information Technology Governance: A Case Study and Leadership Model. University of Phoenix, ProQuest, UMI Dissertations Publishing.
Cyber Security Academy; Wat kunt u verwachten? Den Haag 2013 (www.csacademy.nl,)
Cybersecuritybeeld Nederland CSBN3 (2013). Rapport van het Nationaal Cybersecurity Centrum Nederland.
Defending yesterday: Key findings from The Global State of Information Security® Survey 2014. Advisory Services Security. Price Waterhouse Coopers.
DeFranco, Joanna F. (2013). What Every Engineer Should Know About Cyber Security and Digital Forensics. Taylor and Francis Group, Boca Raton.
Deloitte, Digital infrastructure in the Netherlands, The Third Mainport 2013.
Detica (2011), The Cost of Cyber Crime.
Dialogic (2014), Dé ICT'er bestaat niet: analyse van vraag en aanbod op de Nederlandse ICT-arbeidsmarkt, p. 3.
Endicott-Popovsky, Barbara E. and Viatcheslav M. Popovsky (2014). Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. In: acm InRoads. Vol. 5, No. 1.
European e-Competence Framework 3.0 (2014): http://profiletool.ecompetences.eu/
Financiële Dagblad, Cyberdienst Navo naar Den Haag, 22 maart 2014.
Freed, Sarah Ellen (March 2014). Examination of personality characteristics among cybersecurity and information technology professionals. The University of Tennessee at Chattanooga, Tennessee.
Gabberty, J.W. (2013). Educating the next generation of computer security professionals: the rise and relevance of professional certifications. In: Review of business information systems – Third quarter 2013, volume 17, number 3.
Gabberty, James W. (2013). Educating The Next Generation Of Computer Security Professionals: The Rise And Relevancy Of Professional Certifications. Review of Business Information Systems . In: Vol. 17 Issue 3, p85-98. 14p.
Geers, K (2011) Strategic Cyber Security. NATO Cooperative Cyber Defense Centre for Excellence. Tallinn, Estonia.
Gillebaard, H. et al (2014). Dé ICT'er bestaat niet: analyse van vraag en aanbod op de Nederlandse ICT-arbeidsmarkt. Van: DIALOGIC Innovatie - interactie; in opdracht van ECP, Nederland ICT, CIO Platform Nederland.
Gillebaard, H. et al (2014). Dé ICT'er bestaat niet: analyse van vraag en aanbod op de Nederlandse ICT-arbeidsmarkt. Van: DIALOGIC Innovatie - interactie; in opdracht van ECP, Nederland ICT, CIO Platform Nederland.
Graham R.A., R. Olson & R. Howard (2013), Cyber Security Essentials, Auerbach Publications.
Groeien door veiligheid: een onderzoek naar de waarde van een veilige en betrouwbare ICT-infrastructuur voor de Nederlandse economie"- Ernst & Young, 2011.
Hathaway, M. & A. Klimburg (2012). Preliminary Considerations: On National Cyber Security. National Cyber Security Framework Manual.
Holt, T. (2012). Exploring the Intersections of Technology, Crime, and Terror: Terrorism and Political Violence. Volume 24, Issue 2. Special Issue: Intersections of Crime and Terror.
Holt, T. (2012). Exploring the Intersections of Technology, Crime, and Terror: Terrorism and Political Violence. Volume 24, Issue 2. Special Issue: Intersections of Crime and Terror.
Holt, T.J. & A.M. Bossler (2014). An Assessment of the Current State of Cybercrime Scholarship. In: Deviant Behavior. Volume 35, Issue 1.
Homeland Security Advisory Council, Cyberskills Task Force report, Department of Homeland Security, 2012.
Hoogenboom, B. (2012), Cyber Security Dialogen.
http://csrc.nist.gov/nice/framework/
http://digizine.fd.nl/outlook-special-april2014/

http://ec.europa.eu/justice/data-protection/
http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342
http://www.beschermjebedrijf.nl/
http://www.boomlemmatijdschriften.nl/tijdschrift/tijdschriftcriminologie/2013/4 (losse artikelen zijn te downloaden).
http://www.ictmarktmonitor.nl/ict-marktmonitor-2014/arbeidsmarkt/#2 :
http://www.ictmarktmonitor.nl/ict-marktmonitor-2014/nieuwe-technologieen/#5
http://www.persberichten.com/persbericht/78450/Onderzoek-McAfee-cybercriminaliteit-kost-de-Nederlandse-economie-jaarlijks-ruim-8-8-miljard-euro:
http://www.rijksoverheid.nl/onderwerpen/cybercrime/cybercriminaliteit-bestrijden/responsible-disclosure
http://www.sociosite.org/cyberoorlog.php
http://www.trendsinveiligheid.nl/
Huberts, L.W.J.C. en Naeye, Integriteit van de politie, State- of- the- art van kennis en inzichten, Zeist 2005.
ICT Office 2012.
Justitiële Verkenningen, Aflevering 1, 2012. Themanummer Veiligheid in Cyberspace (losse artikelen zijn te downloaden).
Kabinetsstandpunt inzake Doe Democratie 9 juli 2013-0000395433, 2013.
Kansal, Adarsh; Sikka, Ankit (2014). Awareness On Cyber Crime. In: International Journal of Computer Science and Management Research (Vol 3 Issue 3). Mahamaya Technical University, Ankit Gupta Dronacharya college of engineering, Greater Noida (U.P), India.
Kellermann, Tom (2010), Building a foundation for global cybercrime law enforcement, in: Computer Fraud & Security, 2010, Vol.2010(5), pp.5-8 [Peer Reviewed Journal].
Kessler, G. C., & Ramsay, J. (2013). Paradigms for Cybersecurity Education in a Homeland Security Program. In: Scholarly Commons Citation, Journal of Homeland Security Education, 2. Embry-Riddle Aeronautical University - Daytona Beach.
Kessler, G.C. & Ramsay, J. (2013). Paradigms for Cybersecurity Education in a Homeland Security Program, Journal of Homeland Security Education, 2.
Kessler, G.C. and Ramsay, J.D. (2014) A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students. In: System Sciences (HICSS), 47th Hawaii International Conference on System Sciences. Embry-Riddle Aeronaut. Univ., Daytona Beach, Florida, USA.
Klimburg, A (2012). National cyber security framework manual, NAVO CCD COE.
KNAW Rapport "Digitale geletterdheid in het voortgezet onderwijs", via www.knaw.nl
Kraemer-Mbula, Erika ; Tang, Puay ; Rush, Howard (2012), The cybercrime ecosystem: Online innovation in the shadows? In: Technological Forecasting & Social Change [Peer Reviewed Journal].
Ksherti, Nir; Murugesan, San (2013). EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers. In: Computer, vol. 46, no10, pp. 84-88.
Leukfeldt, R. & W. Stol (2012)(eds.), Cyber Safety: an Introduction, Eleven publishers international.
Manson, D. and R. Pike (2014). The case for depth in cybersecurity education. In: ACM Inroads. Vol. 5, No. 1.
Martin, K. en Panhuis van P., Evaluatieonderzoek naar de leergang Recherchekunde voor zij-instromers, Apeldoorn/Zutphen 2008.
McGettrick, A. (2013). Toward Curricular Guidelines Cybersecurity, Association for Computing Machinery (supported by National Science Foundation). Retrieved from: http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf
Meulen, N.S. van der (2011a). Financial Identity Theft: Context, Challenges and Countermeasures. The Hague: TMC Asser Press.
Meulen, N.S. van der (2011b), Between Awareness and Ability: Consumers and Financial Identity Theft. Communications & Strategies, No. 81: 23 − 44.
Meulen, N.S. van der (2013) Following in the footsteps of terrorism? Cybersecurity as a crowded policy implementation space, Canadian Foreign Policy Journal, 19:2, 123-126, DOI: 10.1080/11926422.2013.773543.

Meulen, N.S. van der (2013a), Following in the Footsteps of Terrorism, Canadian Journal of Foreign Policy, Vol. 19 (2), p. 123- 126.
Meulen, N.S. van der (2013b), DigiNotar: Dissecting the First Dutch Digital Disaster, Journal of Strategic Security Vol. 6, Issue 4.
Meulen, N.S. van der, Lodder, A.R., (2014), Cybersecurity (hoofdstuk 13), in: S. van der Hof, A.R. Lodder, G.J. Zwenne (Ed.), Recht en Computer (6e druk) (pp. 301-318). Deventer: Kluwer.
Meulen, Nicole S. van der, Between Awareness and Ability: Consumers and Financial Identity Theft (March 21, 2011). Communications and Strategies, No. 81, pp. 23-44, 2011. Available at SSRN: http://ssrn.com/abstract=2020214
Meyer, T.T. (2014). Careers in Computer Forensics. Rosen Publishing Group, New York, USA.
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Werken in de publieke sector, Feiten en cijfers 2012, Den Haag 2012.
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De grote uittocht, negen essays over de arbeidsmarkt van de onderwijs- en overheidssectoren, Den Haag 2010.
Ministerie van Buitenlandse Zaken, Kamerbrief Internationale Veiligheidsstrategie, 21 juni 2013.
Ministerie van Veiligheid en Justitie (2013). Nationale Cybersecurity Strategie 2 - Van bewust naar bekwaam, Kamerstuk II 2013-2014, 26643, nr. 291, Den Haag p. 9-35.
Ministerie van Veiligheid en Justitie, Cybersecurity Strategie 2, Van bewust naar bekwaam, Kamerstuk II 2013-2014, 26643, nr. 291 Den Haag 2013 p. 9-35.
Ministerie van Veiligheid en Justitie, Kamerstuk I 2013-2014, 33750.
Ministerie van Veiligheid en Justitie, Verslag van de informele bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 18-19 juli, Vilnius 2013.
Mowbray, Thomas J. (2013). Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions. Publ. John Wiley and Sons.
National Initiative for Cybersecurity Education (NICE) (2011). National cybersecurity workforce framework. Retrieved from: http://csrc.nist.gov/nice/framework/
National Research Council (2013). Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making. The National Academies Press, Washington, D.C.
NCSC (2013). Continuïteit van Onlinediensten, FS 2013-01.
NCSC, (2013), Cyber Security Perspectives 2013.
Nederland ICT (2014), ICT Marktmonitor: http://www.ictmarktmonitor.nl/
Nederland ICT, ICT- Marktmonitor 2013, Hoofdstuk 4 Arbeidsmarkt, 2013.
NICE, National cybersecurity framework workforce. NICCS:
NRC Checkt beoordeeld deze inschatting echter als ongefundeerd: http://www.nrcnext.nl/blog/2012/05/01/next-checkt-%E2%80%98cybercrime-kost-nederland-jaarlijks-zeker-10-miljard%E2%80%99/
O'Connell, M.E. (2012), Cybersecurity without Cyberwar, J Conflict Security Law (Summer 2012) 17 (2): 187-209.
OECD 2012, Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.
Pierre Audoin Consultants (2013), Competitive analysis of the UK cyber security sector.
Pike, R.E. and Curl (2013). The "Ethics" of Teaching Ethical Hacking. Proceedings of the Information Systems Educators Conference, San Antonio, Texas, USA. ISSN: 2167-1435.
Politieacademie, Hoe blauw is de arbeidsmarkt? Een verkenning van het instroompotentieel voor initiële politiefuncties, Apeldoorn, 2012.
Politieacademie, Hoogopgeleiden bij de politie, Een verkenning naar de wervingskansen, Apeldoorn, 2013.
PvIB, QIS, (2014), Beroepsprofielen Informatiebeveiliging.
RAND (2013), Cyber-security threat characterisation: A rapid comparative analysis.

Razzaq, Abdul; Hur, Ali; Ahmad H Farooq; Masood, Muddassar. Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. Paper 2013 for the IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS) in Mexico City, Mexico.
Reich, P. C.; Weinstein, S.; Wild, C.; Cabanlong, A. S. (2010), Cyber warfare: a review of theories, law, policies, actual incidents - and the dilemma of anonymity, in: European Journal of Law and Technology, May, 2010, Vol.1(2) [Peer Reviewed Journal]
Rid, T. (2013), Cyber War Will Not Take Place, C Hurst & Co Publishers Ltd.
Rijksoverheid, Nationaal trendrapport Cybercrime en Digitale Veiligheid 2010.
Rijksoverheid, Strategie Nationale Veiligheid Bevindingenrapportage 2010 en 2012.
Sargent, T.J. Rational Expectations and Inflation, Harper en Row, New York, 1986.
Schmidt, M.N. (ed.) (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare Cambridge University Press.
Schneider, Fred B. (2013). Cybersecurity Education in Universities. IEEE Security & Privacy, Vol. July/Aug 2013. IEEE Computer Society.
Sempere, Carlos Martí (2011), The European Security Industry. A Research Agenda, in: Defence and Peace Economics, 2011, Vol.22(2), p.245-264 [Peer Reviewed Journal]
Siow, A, Occupational choice under uncertainty, Econometrica, p. 631, 1984.
Smith, G. E.; Watson, K. J.; Baker, W. H.; Pokorski Ii, J. A. (2007), A critical balance: collaboration and security in the IT-enabled supply chain, in: International Journal of Production Research, 2007, Vol.45(11), p.2595-2613 [Peer Reviewed Journal].
Sociaal Economisch Onderzoek, Monitor Technische Arbeidsmarkt 2013, Amsterdam 2013.
Solms, R. von & J. van Niekerk (2013). From Information Security to Cyber Security, Computers & Security, in press.
Spidalieri, F. (2013). Joint Professional Military Education Institutions in an Age of Cyber Threat. Report from the Pell Center for International Relations and Public Policy.
Spruit, M. en F. van Noord (2014). Beroepsprofielen Informatiebeveiliging. In opdracht van PvIB en QIS.
Spruit, M. en Noord van F, Onderzoek naar kwalificatie en certificatie van informatiebeveiligers, Zoetermeer 2011.
Stol, W. & J. Janssen (2013). Cybercrime and the Police. Boom Lemma, Utrecht.
Symantec, 2012. 2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually [online]. Available from: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 [Accessed 10 December 2012].
Tanner, A. (2014). Examining the Need for a Cyber Intelligence Discipline. Angelo State University, Center for Security Studies Examining the Need for a Cyber Intelligence Discipline. Journal of Homeland and National Security Perspectives 1:1.
Themanummer Tijdschrift voor Criminologie: Criminaliteit en Internet (Van Erp, Stol, & Van Wilsem).
TNO (2014). CyberSecurity Perspectives 2013. Jaarlijks Security Report van KPN NL, KLPD, TNO, NCSC.
UWV (2014). Sectorbeschrijving Informatie en Communicatie
Van Aartsen, J, Toespraak bij de opening van het European Cybercrime Centre (EC3) op 11 januari 2013, Den Haag 2013.
Van den Berg, Jan, Van Zoggel, Jacqueline, Snels, Mireille, Van Leeuwen, Mark, Boeke, Sergei, Van de Koppen, Leo, Van der Lubbe, Jan, Van den Berg, Bibi, De Bos, Tony, (2014), On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security EducationBerg, J. van den (juli 2014). PPT-presentatie 'Cyber Security Academy (CSA) The Hague: https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf
Verbond van Verzekeraars (2013), Position paper: Virtuele risico's, echte schade; Over het verzekeren van cyberrisico's.
Verbond van Verzekeraars (2013), Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's.

Verslag van de informele bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 18-19 juli 2013 te Vilnius.
White House (2011). International Strategy for Cyberspace, beschikbaar op: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy for_cyberspace.pdf.
WRR, (2011), iOverheid.

Bijlage 2: Overzicht geraadpleegde organisaties

Interviews met publieke en private organisaties

Organisatie	Naam
Platform voor Informatie Beveiliging	Marcel Spruit Fred van Noord
The Hague Cyber Security Academy	Jacqueline van Zoggel
Nationaal Cyber Security Centrum	Aart Jochem
Cyber Security Raad	Gerben Klein Baltink
KLPD	Roxanne Rotgers Team lid Team High Tech Crime, Landelijk eenheid Politie
ECABO	Hans Blankendaal
Deloitte	Marko van Zwam Willem van der Valk Jochem van Kerkwijk Henri Hambartsumyan
AMC	Jelmar Halma
Nederlandse Vereniging van Banken	Remco Ruiter
Verbond van Verzekeraars	Jos Schaffers
Bol.com	Raymond van den Hoek
Criminologie, Universiteit Leiden	Johan van Wilsem
RET	Hugo Leisink
ProRail	Stoffel Bos
Gemeente Den Haag	Jilles van Harselaar Karin van Poelgeest
EPZ	John Geers
Rabobank	Mark Beerends Henk Jan Esterik
Fox-IT	Walter Doorduin
WeSecureIT	Wouter Parent
KPN	Martijn van der Heide
Ministerie van Defensie	Kraesten Arnold Hans den Biggelaar Geran Kuijs
Gemeente Utrecht	Kaj Siekman
Ordina	Wouter-Bas van der Vegt
Atos	Paul Oor
Exact	Fred Streefland

Interviews met opleiders

Opleiding	Opleidingsaanbieder	Naam
WO breed:		
Bachelor Informatica	Universiteit van Amsterdam	Robert Bellema
Computer Engineering (interview over al het cyberonderwijs van de faculteit Informatica)	TU Delft	Jan van der Lubbe
Computer Science, master 'Computer Security'	Kerckhoffs Instituut (= samenwerkingsverband Radboud Universiteit Nijmegen, Technische Universiteit Eindhoven en Universiteit Twente)	Lejla Batina
Computer Science, master 'Computational Science' (en masters 'Computer Science', 'Software Engineering', System and Network Engineering', 'Information Studies / Sciences')	Vrije Universiteit Amsterdam, deels in samenwerking met Universiteit van Amsterdam	Alban Ponse
Computer Science & engineering (Master)	TU Delft	Emile Hendriks
Cyber Security Academy, Den Haag	Cyber Security Academy, Den Haag	Mireille Snels
WO sectorspecifiek:		
Rechten, master 'Law and Technology'	Universiteit Tilburg	Colette Cuijpers
Military Strategic Studies, master 'Intelligence & Security'	Nederlandse Defensie Academie	Paul Ducheine
HBO breed:		
Security management	Saxion Apeldoorn	Trijntje Dijkstra
Information security management	Haagse Hogeschool, Zoetermeer	Marjolein Faassen
Bachelor Informatica met 'studieroute Cybersecurity'	Fontys	Casper Schellekens
MBO breed:		
Beroepsrichting ICT- en mediabeheer, uitstroomrichting ICT-beheerder	ROC van Twente	Vincent Blokhuis
Beroepsrichting ICT- en mediabeheer, uitstroomrichting Netwerkbeheerder		
Beroepsrichting Applicatie- en mediaontwikkeling, uitstroomrichting Applicatieontwikkelaar		
Medewerker beheer ICT		

Opleiding	Opleidingsaanbieder	Naam
Digitaal onderzoeker (opleiding bestaat niet meer)	ROC Midden Nederland	Onno Hardebol
MBO sectorspecifiek:		
Opleiding Veiligheid en vakmanschap, vakrichting ICT	Nederlandse Defensie Academie	Jordi Palte, Koning Willem I college
Private / in company opleidingen:		
Business & IT	Nyenrode Business University	Loes van Kempen
Trainingen op het gebied van o.a.: - cybersecurity algemeen: CISSP-, SABSA-, CISA- en CISM-certificering ; - Software Lifecycle Security; - certificering t.a.v. informatiebeveiliging.	Cap Gemini	Frank Geerling
Trainingen op het gebied van informatiebeveiliging, o.a.: - CISM-certificering - 5-daagse opleiding Advanced Crash Course Cyber Security - 6-daagse verkorte opleiding Informatiebeveiliging - 5-daagse opleiding Informatiebeveiliging in de Zorg	IIR / ICT Academy	Michel de Coninck
In company trainingen 'IT governance & security'	Pink Elephant Academy	Fleur van der Wal

Bijlage 3: Bijeenkomst Experts

Doel van de bijeenkomst

Doel van de bijeenkomst was de bevindingen uit het onderzoek terug te koppelen aan een brede groep stakeholders en de (praktische) betekenis van de belangrijkste onderzoeksuitkomsten te bespreken. De centrale vraag daarbij was: Wat is nodig om in de toekomst een duurzame, goede match te realiseren tussen vraag en aanbod van Cyber Security Professionals.

Deelnemers

Ruim vijfentwintig experts, gelijk verdeeld over publieke- en private organisaties en onderwijs- en opleidingsorganisaties waren voor deze bijeenkomst uitgenodigd. Hoewel alle benaderde experts zich zeer geïnteresseerd toonden in het onderzoek waren uiteindelijk slechts zeven van hen daadwerkelijk in de gelegenheid om deel te nemen. In deze groep waren alle relevante perspectieven vertegenwoordigd (HR-managers, beleidsontwikkelaars en -adviseurs, onderwijs- en opleidingsmanagers).

Aan de expertgroep namen deel:
Mark Beerends (RABO)
Soenil Choenni (WODC)
Douwe Grijpstra (Panteia)
Leo van Koppen (Haagse Hogeschool))
Paul Oor (Atos)
Hugo Leisink (RET)
Johan van Wilsem

Vanuit het onderzoeksteam:
Simon Broek
Bert Jan Buiskool
Jaap van Lakerveld
Ingeborg Tönis

Programma en werkwijze

Het programma was opgezet volgens de *Delphi methode.* Een belangrijk kenmerk van deze methode is de herhaalde raadpleging van deskundigen waarbij de resultaten tussentijds worden gerapporteerd. Dit vormt dan weer de inzet voor een nieuwe ronde raadpleging enzovoorts. Opeenvolgende rondes van raadplegen van experts bouwen zo op elkaar voort.
Tijdens de bijeenkomst is de Delphi methode op de volgende manier toegepast:

- Bevindingen uit het onderzoek tot dan toe werden voorgelegd aan alle deelnemers. Hierbij stonden de gevonden discrepanties en intransparanties t.a.v. de vier onderscheiden functiegroepen centraal:
  a) technisch dominante specialistische cybersecurityfuncties;
  b) niet technisch dominante specialistische cybersecurityfuncties;
  c) technisch dominante functies waarbij cybersecurity een onderdeel is;
  d) niet technisch dominante functies waarbij cybersecurity een onderdeel is.
- In twee subgroepen zijn mogelijke oplossingsrichtingen aangedragen.
- De gegenereerde oplossingsrichtingen werden voor alle deelnemers zichtbaar gemaakt. Zo ontstond een totaalbeeld van oplossingsrichtingen waarop experts vervolgens reflecteerden.
- Tot slot vond ranking van oplossingsrichtingen plaats.

Bij het genereren van oplossingsrichtingen ging het om oplossingsrichtingen ten aanzien van:

a. het op de korte en langere termijn voldoen aan de vraag naar functies binnen de hierboven onderscheiden functieprofielen;
b. transversale (functieprofiel overstijgende en –doorsnijdende) kwesties die een rol spelen bij het realiseren van een optimale match vraag en aanbod.

Opbrengst

Tijdens de bijeenkomst is met veel inzet en enthousiasme gesproken over de oplossingsrichtingen. Relatief veel support was er voor de oplossingen zoals als het stimuleren van loopbaan switches (personeel omscholen en inzetten in cybersecurity posities); datawetgeving als stimulans om cybersecurity op de kaart te zetten en serieus te nemen; bewustwordingscampagnes onder brede groepen van personeel en burgers. Daarbij werd benadrukt dat cybersecurity eigenlijk beschouwd moet worden als een competentie die ieder zich afhankelijk van rol en positie in enigerlei, of hoge mate eigen moet maken. Ook de vergroting van de transparantie van het onderwijs en opleidingen aanbod werden veelvuldig genoemd. Het scheppen van adequate arbeidsvoorwaarden ten behoeve van het aantrekken van vrouwen in het beroep, had prioriteit voor de helft van de groep. Weliswaar genoemd, maar met minder prioriteit waren de oplossingsrichtingen: andere wervingsvormen dan vacatureadvertenties benutten; meer aandacht voor cybersecurity in generieke opleidingen en gericht post-initieel opleiden van mensen.

De oplossingsrichtingen die in de bijeenkomst met experts naar voren kwamen, zijn in samenhang met oplossingsrichtingen uit de interviews en de analyse door de onderzoekers verwerkt in hoofdstuk 5 van dit onderzoeksrapport.

Bijlage 4: Summary

Reason and purpose of the study

A shortage of Cyber Security Professionals (CSPs) is a great vulnerability to the resilience of the vital sectors. In the "National Cyber Security Strategy 2 (NCSS2): From awareness to capability" (2013), it is emphasized that the Government wishes to have sufficient cyber security knowledge and skills. In this context, it is important that in the short and (medium) long term, there is a balance between demand and supply on the labor market for CSPs in private and public organizations. For this reason, the National Coordinator for Security and Counterterrorism (NCTV) wants to gain insight into the nature and scope of a (possible) shortage of these professionals (both technical and non-technical) and identify solutions in order to reduce these possible shortages in the short and (medium) long term. In this context, PLATO BV of the University of Leiden has conducted a labor market study into the demand and supply of Cyber Security Professionals in cooperation with Ockham IPS. This study is commissioned by the Research and Documentation Center (WODC).

Research questions

The following research questions are central to this study:

- To what extent can a possible qualitative and quantitative shortage of Cyber Security Professionals at higher and secondary level be expected, now and in future?
- How could these shortages in the existing and future labour market for Cyber Security Professionals be solved?

Study design and approach

In this research, the labour market for CSPs will be approached as a domain in which supply of and demand for professionals in the area of cyber security come together and (try to) find each other. In terms of gaining insight into the demand, the focus in this study is on vacancy analysis. In terms of the supply side, the study focuses on the education and training opportunities.

To gain answers to the research questions from various relevant perspectives and sources, other research methods have been used too. The study consisted of the following, partly overlapping components:

- Literature study into cyber security, the work field, characteristics and job profiles of CSPs. This included policy literature and academic literature, both Dutch and international literature.
- Analyses of the social context and developments (politically, economically, socially, technologically and legally) that influence the supply of and demand for CSPs.
- Vacancy research (with the help of vacancy spider Job feed[107] of Text kernel).
- Inventory and analyses of the education and training opportunities and inventory of the numbers of students. In this context, internet research has been conducted and 18 education providers have been consulted (by means of 18 interviews, partly face-to-face and partly by telephone).
- Preliminary and in-depth interviews (partly face-to-face and partly by telephone) with employers and employees in the private and public domain. In total, there were 34 interviews spread across 25 organizations.
- Expert meeting. This meeting was held in the final stages of the study, with the aim of discussing the discrepancies found between supply and demand as well as areas in which solutions may be found. Seven participants of these various organizations were involved in the expert meeting.

[107] http://www.jobfeed.nl/

Cyber security

Cyber security is a rather ambiguous concept. The various definitions of cyber security found in literature often emphasize information security and IT. Cyber security should not be interpreted too restrictively. The term cyber security refers to the vulnerability of companies, citizens, government and society as a whole. These vulnerabilities as well as their solutions have both technical IT aspects and interactive (human-IT) aspects. This is what makes cyber security an organizational issue in addition to a technical issue.

Conclusion 1: Cyber security is both an IT and an organizational issue. Most of all, cyber security should be seen from a wider organizational perspective in which various roles and tasks are to be fulfilled.

The work field of Cyber Security Professionals

The work field of the Cyber Security Professional is strongly subject to change. The rapidly changing digital world with its threats and essential safety criteria sets high standards for public and private organizations being or becoming cyber secure. Both the frequency and the impact of incidents, in terms of direct and indirect damages (such as reputational damage), are increasing. Companies and public organizations are more and more aware of the fact that cyber security is not just an IT issue; it is an integral theme. Cyber security has gone from an IT issue to a 'boardroom issue,' because the survival of the company could be at stake. Growing policy attention to cyber security, the necessity to be aware of the risks (since the internet is present in all areas of daily life) and changes in legislation (with regard to privacy and data protection) have an additional driving effect on the development of demand.

Conclusion 2: Two factors keep the work field of the Cyber Security Professional rapidly changing. On the one hand, it is about societal developments (at political, economic, social, technical and judicial level). On the other hand, incidents (depending on the frequency and impact) call for adjustments in the work field.

Position groups

In the literature, three dimensions emerge on which the positions of Cyber Security Professionals can be described:

- Work activities can be classified as technically dominant or not technically dominant. Technically dominant implies that the focus is on the IT perspective. The not technically dominant positions focus more on the organizational perspective.
- The position can be specifically focused on cyber security or have cyber security as a component.
- The position can be oriented operational-tactically or tactical-strategically.

Based on these dimensions and on the analysis of vacancy descriptions, four position groups may be distinguished:

1) *Technically dominant specialist cyber-security positions*. These positions are focused very specifically on IT/information security and have a large technical component. Examples of positions are ethical hackers, penetration testers, software testers and technical security engineers.
2) *Not technically dominant specialist cyber-security positions*. These cyber security specialists look at security more from an organizational perspective. Job examples are IT security officers, IT security specialists, security officers, information security officers.

3) *Technically dominant positions of which cyber security is a component*. These professions are technical in nature but not specialized in cyber security. This is a large group of professions that require or preferably require a cyber-security related certificate. Job examples are system operators, software developers and architects.
4) *Not technically dominant positions of which cyber security is a component*. This is the least defined position group. It contains numerous positions, such as policy advisors, lawyer, directors and auditors. With these positions, cyber security can be subject of the core activity (for example, a lawyer specialized in privacy issues or a policy advisor in the field of cyber security). Furthermore, it concerns positions that view cyber security as part another domain rather than as core of the work (for example, part of policy making, jurisdiction).

The distinction operational-tactical and tactical-strategic is reflected in all four position groups.

Conclusion 3: Based on the literary and analysis of vacancy descriptions, four position groups are distinguished for the Cyber Security Professional that may be used in relation to labour market research:
- *Technically dominant specialist cyber-security positions.*
- *Not technically dominant specialist cyber-security positions.*
- *Technically dominant positions of which cyber security is a component.*
- *Not technically dominant positions of which cyber security is a component.*

The demand for Cyber Security Professionals and the total CSP employment

In the first three quarters of 2014, a total of 916 vacancies have been published related to the security domain. On an annual basis (during the last quarter of 2013 and the first three quarters of 2014) there were 1,158 published vacancies in the field of cyber security. The total demand will be higher, because informal recruitment channels and challenges[108] aimed at recruitment do not count as vacancies in the vacancy analysis.
To get an impression of total employment (the total number of jobs) in the security domain, we draw a comparison with the number of published vacancies and employment in the broader IT sector. In the broad IT sector, one vacancy equals six jobs.[109] If we apply the same relationship between vacancies and jobs in the security domain, the total employment in the security domain is estimated at 7,000 jobs based on this.

Based on the environmental analyses (the societal interest and the role of incidents increase, see conclusion 2), it is expected that the demand for Cyber Security Professionals will increase. On the one hand, the urgency to apply knowledge and skills in this field increases. On the other hand, the cyber-security domain is increasingly seen as an organizational and as a multidisciplinary matter.
The expected rise in demand applies to all four position groups as well as to adjacent positions. The cyber domain is an important part of life, which is why various adjacent positions in which knowledge of cyber security is indispensable, are necessary.
A distinction must be made between the demand in positions at the level of Upper Secondary Vocational Education, Higher Vocational Education and University. Because of digitization and automation, the demand for professionals with Uppper secondary Voca-

[108] A 'challenge' in this study is referring to a recruitment activity with a *gaming* character during which issues related to cyber security must be solved.
[109] In 2013, total employment in the IT/automation sector was approximately 300,000 (Panteia based on P-Direkt and Dutch Labour Force Survey, Statistics Netherlands). The total number of vacancies on an annual basis is approximately 50,000 (Panteia/PLATO based on vacancy analysis Job Feed). The ratio between the number of vacancies and total employment is therefore 1 : 6.

tional Education is decreasing, whereas the demand for higher educated professionals is increasing.

Conclusion 4: Even though the number of visible vacancies is still modest, there are indications (increase in urgency and a broader interpretation of the cyber-security domain) that the demand for CSPs (in its totality) will increase in the future. The increase will mainly apply to higher educated professionals and less to professionals with Upper Secondary Vocational Education.

The nature of the demand for the four position groups as identified in this study may best be defined as follows:

1) *Technically dominant specialist cyber-security positions*. Aside from big employers (banks, police and defence), the labour market for this profile is dominated by consultancy companies. These specialists (hackers, penetration testers) share the role of front-runner in the development of cyber security with cyber criminals. In order to keep up with the technological developments of cybercrime, the demand for these specialists will rise steadily.
2) *Not technically dominant specialist cyber-security positions*. The labour market for this position profile has a more diverse range of demanding organizations. Hiring this type of CSP is the first step for many organizations to straightening out cyber security. In many cases, one CSP is sufficient for organizing the security. Specialist tasks are performed by hiring a third party. After strong growth in the first five years, the demand for not technically dominant specialist cyber-security positions will decline lightly, because organizations have embedded cyber security in their organizations. At that point, however, the replacement demand will also start to play a role in the development of demand. Vacancies in relation to this position group often ask for experienced people.
3) *Technically dominant positions of which cyber security is a component*. In the labour market for this position group, the highest increase in demand is expected. This market is dominated by software developers. In recent years, these companies have been committed to improved security of their software (secure by design) and they demand IT people with experience in the domain of security, security certificates or security affinity. Since a growing number of organizations can be seen as software companies (IT is the core of many companies), the demand for these technicians increases in future. The demand for safer systems resonates in the system development and system management.
4) *Not technically dominant positions of which cyber security is a component*. The labour market for this position profile has a multitude of different positions, and some professionals might not even realize that they deal with cyber security. In future, competences regarding cyber security-related tasks will be asked more often and more explicitly.

Conclusion 5: An increase in the demand applies to all position groups, but the largest growth is expected in the technically dominant positions of which cyber security is a component.

Supply of Cyber Security Professionals from education and training

In this research, over eighty different types of supply have been inventoried. If the number of supply locations is incorporated, it involves many hundreds of training programs and other forms of supply. The training supply related to cyber security is extremely varied and extensive. Many forms of education co-exist, such as graduate and post-graduate programs, short courses, master classes, workshops, seminars, learning through practice, distance learning and in-company training.
The trainings are offered on numerous locations. There are graduate and post-graduate programs from Upper Secondary Vocational Education to University. In the private sector, the supply is huge as well. The focus here is on keeping the knowledge and skills of working professionals up-to-date. With regard to the content and depth, the supply is varied as well. This includes educational programs with clear technical and IT contents as well as programs with clear security, legal or forensic contents. There are also programs that train participants indirectly but in-depth in courses and competences relevant to cyber security. This category includes educational programs that have a strong IT component, but that focus on areas other than technology or security, such as artificial intelligence, methods and technologies studies, medical information technology, logistics, measuring and regulations technology, etc. In conclusion, there is a much wider range of educational programs that contribute to students' knowledge and skills other than the programs directly aimed at IT, or internet and cyber security.

The multitude of courses, educational programs and other forms of supply, however, also lead to lack of transparency of the supply. Information about educational programs and processes are retrievable, but no clear overview of the educational possibilities in relation to the competences in which participants want to and/or have to be educated exists.

Conclusion 6: The educational supply regarding cyber security is varied and extensive. Educational programs are often offered on various locations and there is much variation in types of education or training. At the same time, the supply is not transparent.

Regarding the supply of professionals from education and training, a sufficient number of participants seem to be in a relevant training program in 2014:

- An inflow of 6,880 students at Upper secondary Vocational Education level 4;
- An inflow of 73 students at Higher Vocational Education associated degree level;
- An inflow of 4,053 students at Higher Vocational Education level;
- An inflow of 292 students at Master level;
- An inflow of at least 200 participants in post academic and post-executive Masters (as appears from the interviews).

Therefore, there is a great potential of people who appear to be employable in principle. Even if we take into account a dropout rate of 50%, the numbers remain high compared to the available vacancies. At the same time, these numbers only lead to an inflow into cyber security related positions to a very limited extent. Upper secondary Vocational Education students often continue their studies in Higher Vocational Education. Many broader Higher Vocational Education and University programs have included cyber security in their programs to a limited extent only, and there are only few specialist cybersecurity programs. This means that students do not, or only relatively late, include cyber security as an option in their studies or career.

Conclusion 7: The education potential is, in principle, sufficient to meet the demand for CSPs. The question is whether participants in cyber security related programs view cyber security as a possible career option.

Found discrepancies between supply and demand

Found discrepancies at research question 1: To what extent can a possible qualitative and quantitative shortage of Cyber Security Professionals at higher and secondary level be expected, now and in future?

In the relation between the supply of and demand for CSPs, lack of transparency and qualitative discrepancies can be ascertained rather than quantitative discrepancies. The challenge lies not in educating more people, but in sparking people's interests in cyber security and jobs in said area during their education. The problems in connectivity (discrepancies between supply and demand) that organizations experience are of a qualitative nature rather than of a quantitative nature, or they are a result of a lack of transparency of the labour market. In short, the following discrepancies arise:

- While students are trained in areas relevant to cyber security, they miss a specific focus on cyber security.
- Many organizations have insufficient knowledge about what they need, who they look for and where to find them.
- There is sufficient supply; however, the professionals do not have the desired level of expertise yet. They lack (depending on the position and tasks) either the technical knowledge or the organizational knowledge.
- Professionals have gotten cyber security as an additional subtask, but they are not specifically trained in that area. Since they have many other tasks, rapid development of competences in the field of cyber security is not easily done.

Conclusion 8: Quantitatively, there is no shortage in the supply. The match between the demand for CSPs and the supply of these professionals is obstructed by qualitative discrepancies and a lack of transparency.

Solution areas to found discrepancies

This concerns answering the second research question: How could these shortages in the existing and future labour market for Cyber Security Professionals be solved? In other words, how can the match between supply and demand be improved? In the study, the following (also emphasized by experts in the field of cyber security) directions in which solutions may be found emerge:

1. Use the possibilities of education in solving discrepancies.

Education can play a major role in solving discrepancies. This includes raising awareness amongst pupils and students in general, motivating some of these students to make a study selection relevant to cyber security, and providing an even more select group of students with appropriate and expert training. Learning and specializing in a rapidly developing field as cyber security requires a lifelong-learning approach. In the context of lifelong learning, it is important to look for efficient and effective ways to develop and share knowledge in work situations, and to translate that into improvements and innovations. The work environment goes beyond the borders of one's own organization.

Aside from professionalization in the sense of personal development in the profession, there is also the necessity of development in the field. Cyber security is a domain in which much work is done in numerous public and private (small and bigger) organizations and industries at various levels. The educational world also contributes to the developments in the cyber security domain. Collaboration between all parties involved is of vital importance in keeping the cyber security sector and those who work in it up to date. This is demonstrated by the active involvement of IT companies in academic programs, in participation of practitioners as teachers in higher education programs, and in the participation of scientists in solving practical problems.

2. *Change the work processes in organizations and collaboration between organizations in order to upgrade the level of cyber security and maintain it.*

In the study as a whole, the following possibilities have emerged in this regard:

- Create opportunities in and between organizations to share knowledge and to learn from each other;
- Improve secondary employment conditions/benefits, which can make the work more attractive to more groups, such as women;
- More efficient and specific recruitment (also within one's own organization, by pointing out the possibilities of growth in a cyber-security related position to prominent employees);
- Deployment of a pool of professionals from various organizations, outsourcing and hiring external specialists;
- Make visible the work of the CSP within the organization and its use;
- Establish and make use of a less hierarchical organizational structure (applies to larger organizations).

3. *Clarification of education and training paths.*

The relation between training paths, the competences to be acquired, positions to be fulfilled, and positions to be achieved in the labour market is diffuse. The paths that support career developments in cyber security are too. Making choices in the galore of possibilities is not always easy. Both the people concerned and the organizations experience the disadvantages of that. It means that too often, the right man or woman ends up in the wrong place. It leads to inefficient and ineffective training and career paths. Clarification of the education and training paths will have a positive effect on the quality of the supply and the guidance of outflowing participants and students to positions in the field of cyber security. This solution also points towards lifelong learning. The work field of cyber security asks for continuous updating of knowledge and skills. In this regard, the necessity to create and establish a system of maintenance, update and development of knowledge grows.

4. *Monitor developments in society, education and courses, and the labor market. The resulting data can positively influence the match between supply and demand in the short and (medium) long term.*

In line with solution three, data acquisition and registration on study programs and the demand on the labor market can be a usable resource for quality improvement. The study into the labor market for Cyber Security Professionals, as described in this report, provides a state of affairs. Society as a whole and the work field of CSPs are changing rapidly. A form of monitoring of developments in society, the labour market and the education market can contttribute to the match between the demand for and supply of CSPs in the shorter and longer term.

5. *Creating a stronger and more challenging image of the cyber-security work field and positions.*

Cyber security positions are often associated with a specific type of ethical hackers who get lost in their jobs completely (black t-shirts, ponytails etc.). On the other hand, cyber security positions are associated with 'troublemakers in the organization:' because of their focus on everything that could go wrong, they are a bit difficult in the eyes of others. The challenging, progressive and complex aspects of the work may be placed to the forefront. A different issue is that the sector predominantly consists of men. In the domain of cyber security, various positions requiring different types of competences can be fulfilled. This makes the work field interesting for both men and women. A positive image of the possibilities and challenges creates a larger pool. Instructions, courses and public actions (in the form of challenges) could also contribute to change.

6. *Take on cyber security as a common responsibility of citizens, government, organizations and education: aimed at raising awareness.*

All organizations and experts consulted agree: cyber security is a matter that influences the life of almost every citizen. Therefore, it is important to work on raising awareness of society as a whole. The purpose of this is to make everyone aware of the risks and to defend themselves against and of the means to do so. This has resulted in a desire to train and use experts who can reach this broader range of citizens with the message that cyber security calls for alertness, precautions and audits in the field of information security.
This also implies that cyber security should be seen as something that plays a role anywhere anytime people work and interact with IT systems. It is also a task for basic education (primary and secondary education). How this should be shaped will have to be researched in future studies.

Conclusion 9: Solutions for discrepancies in the labor market for CSPs cover:

1. *Use the possibilities of education in the field of, inter alia, raising awareness, study selections, clarification of study paths and opportunities for lifelong learning in the area of cyber security.*
2. *Strengthen and improve work processes in organizations and stimulate collaboration between organizations.*
3. *Clarify study and training paths.*
4. *Monitor developments related to the labor market of CSPs.*
5. *Improve and strengthen the image of the cyber-security work field and the CSP.*
6. *Continue on the chosen path to approach cyber security as a common responsibility of citizens, government, organizations and education: aimed at raising awareness.*