Auteursinformatie: *Prof. dr. ir. Jan van den Berg is hoogleraar Cyber Security aan de Technische Universiteit Delft. Jacqueline van Zoggel is senior adviseur Hoger Onderwijs. Samen vormen zij sinds dit voorjaar de directie van de Stichting Cyber Security Academy The Hague, een samenwerkingsverband van de Technische Universiteit Delft, Universiteit Leiden en De Haagse Hogeschool.* ***Voor meer informatie: www.csacademy.nl***

CYBER SECURITY VRAAGSTUKKEN

Den Haag, stad van vrede, recht en veiligheid, heeft de ambitie geformuleerd uit te groeien tot een internationaal toonaangevende veiligheidsregio. Daarom is afgelopen zomer de netwerkorganisatie The Hague Security Delta (HSD) opgericht, waarin inmiddels zo'n tweehonderd partners uit de gouden driehoek (overheid, bedrijfsleven, kennis-instellingen) zijn verenigd.

In een snel digitaliserende samenleving is goed functionerende en veilige IT (kortweg cyber security) cruciaal voor het reilen en zeilen van de samenleving als geheel. Betrokken HSD-partners zoals ministeries, banken, telecombedrijven, energieleveranciers, adviesbureau's en (inter)nationale koepelorganisaties zoals Europol/EC3, NCTV en kennisinstellingen, voorspellen een groeiende behoefte aan specialisten op het terrein van cyber security. De Technische Universiteit Delft, de Universiteit Leiden en de Haagse Hogeschool hebben hun kennis en kunde gebundeld in de dit voorjaar opgerichte stichting Cyber Security Academy, The Hague (CSA). Op initiatief van de CSA werken enthousiaste wetenschappers en docenten vanuit diverse disciplines samen met experts uit de beroepspraktijk, aan een vernieuwend programma aanbod. Een gloednieuwe wetenschappelijke masteropleiding Cyber Security voor professionals, die dit najaar van start gaat, vormt het eerste concrete resultaat van deze werkzaamheden. Deze postinitiële opleiding leidt op tot een MSc in Cyber Security [1] en kent, als één van de eerste opleidingen in Europa, een integrale benadering van cyber security. De opleiding brengt de technische, juridische, bestuurlijke, economische, politieke en psychologische dimensies van digitale veiligheid met elkaar in verband en gebruikt geïntegreerde benaderingswijzen voor het oplossen van de snel in complexiteit toenemende vraagstukken rond cyber security.

Cyber risico's in perspectief

De groeiende aandacht voor cyber space en cyber security is niet verwonderlijk in een samenleving die in rap tempo nagenoeg al haar vitale processen afhankelijk heeft gemaakt van ICT. Het aantal toepassingen en gebruikers groeit gestaag (bijna drie miljard gebruikers wereldwijd [2]. De technische mogelijkheden kennen een autonome vlucht en de vraag van gebruikers is nagenoeg onbegrensd. Cyber space is daarmee in enkele decennia uitgegroeid tot een complex, manmade

Bowtie model

system met grote afhankelijkheden en tal van dimensies die veel verder reiken dan de technische aspecten alleen.

De ermee gepaard gaande dreigingen en kwetsbaarheden zijn talrijk en leiden tot een gestaag groeiende reeks van incidenten: er gaat vrijwel geen dag voorbij zonder dat een of ander cyberincident de krantenkoppen haalt.

Incidenten zijn vaak het gevolg van bewust uitgevoerde aanvallen die resulteren in incidenten in de sfeer van cyber crime (creditcard fraude, digitale spionage) en cyber warfare (militaire aanvallen met drones, Stuxnet). Ook treden er incidenten op door technische of persoonlijke fouten, als neveneffect van natuurrampen, door bestuurlijk onvermogen, door onvoldoende adequaat toezicht en/of door naïviteit van eindgebruikers.
De concrete impact is verschillend van karakter en kan variëren van economische schade, verstoring van bestuurlijk en politieke verhoudingen, milieuschade tot schendingen van grondrechten en privacy, dan wel combinaties daarvan.

Als gevolg van een complexe verwevenheid van boven-genoemde dreigingen, kwetsbaarheden, incidenten en impact, manifesteren cyber incidenten zich steeds meer als een veelkoppig fenomeen. Het begrip 'risico' als resultante van de kans op incidenten en de impact daarvan op de samenleving is, binnen het door ons gecreëerde nieuwe domein van cyber space, toe aan een grondige herijking.

De constatering lijkt gerechtvaardigd, dat de beheersbaarheid van via het Internet gestuurde systemen en de weerbaarheid van actoren in cyber space (overheden, bedrijven en burgers) momenteel geen gelijke tred kunnen houden met (de enorme snelheid van) de hedendaagse digitale innovaties.

Nog veel (te) weinig aandacht gaat uit naar doordachte preventie en regulering zoals het definiëren van politieke en bestuurlijke verantwoordelijkheden (rol van overheden). Ook preventieve bedrijfsstrategieën (cyber security als onderdeel van ieder van IT- afhankelijk bedrijfsproces) komen nog maar aarzelend tot ontwikkeling, en ten slotte laat de bewustwording en educatie van (eind)gebruikers (de bedrijfscultuur) vaak nog veel te wensen over.

Kortom, er is groeiende noodzaak om gezamenlijk acceptabele cyber risico's te formuleren en toe te werken naar meer integrale vormen van cyber risicomanagement, inclusief adequate wet- en regelgeving, over de volle breedte van de digitale samenleving.

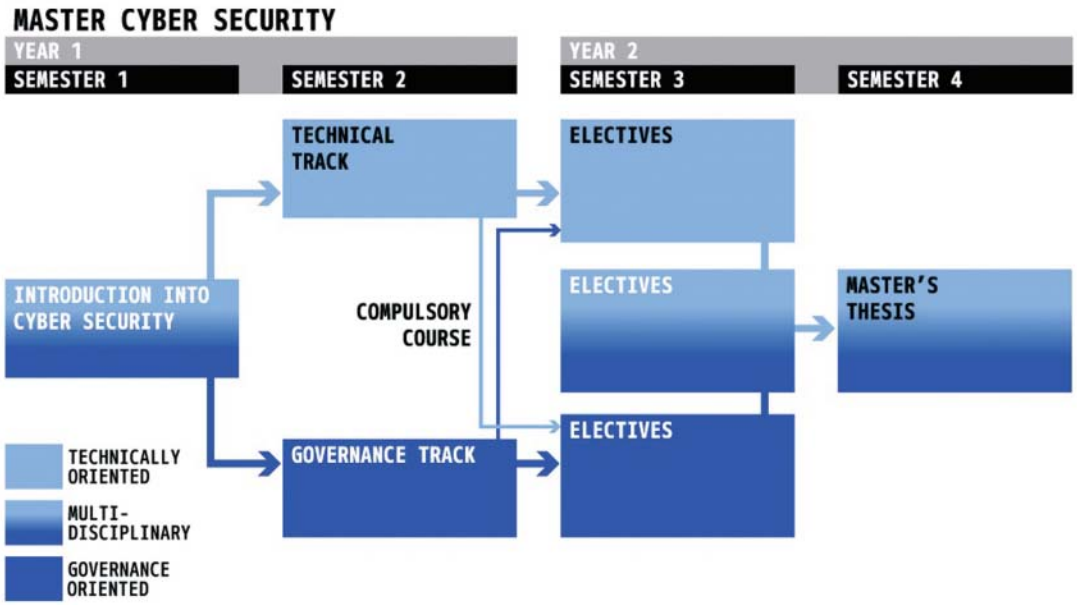
De zich ontwikkelende vraag naar CS-specialisten

Het is niet verwonderlijk dat momenteel de vraag van werkgevers in uiteenlopende sectoren vaak uitgaat naar technisch gekwalificeerd personeel die de werking van IT begrijpen. Deze vraag, naar technisch talent, dat binnen organisaties en bedrijven een zichtbare bijdrage levert aan beter beveiligde (primaire processen) is begrijpelijk. Het is echter

wel een eenzijdige aanpak van problemen, die weinig recht doet aan de complexiteit en de afhankelijkheden die cyber security inmiddels kenmerken. Een aanpak die op termijn mogelijk zelfs een meer visierijke (lees: noodzakelijke nieuwe) benadering in de weg staat. Het is de verwachting van overheidsinstanties [3], kennisinstellingen en experts verenigd in de Cyber Security Academy dat naast de groeiende vraag naar technisch geschoold personeel ook de vraag naar een nieuw type professional met geïntegreerde kennis van en met een visie op het vergroten van de digitale weerbaarheid zal toenemen. Het gaat dan om professionals met overzicht over en (basis)kennis van zowel technische, juridisch/ethische, bestuurlijk/politieke als culturele/psychologische aspecten samenhangend met digitale veiligheid, die in staat zijn op strategisch en tactisch niveau sturing en richting te geven aan nieuwe strategieën en concepten voor de regulering van complexe digitale processen en digitaal verkeer.

Het huidige aanbod aan cyberopleidingen

Een nadere analyse van de hierboven geschetste frictie tussen vraag en aanbod van specialisten cyber security laat het beeld zien van een tot nu toe te gefragmenteerd en op onderdelen tekortschietend opleidingenaanbod in Nederland zowel in kwantitatieve als kwalitatieve zin. Uit een onlangs op initiatief van enkele hoogleraren cyber security opgestelde inventarisatie naar (wettelijk erkend) opleidingenaanbod in het hoger onderwijs in Nederland komt naar voren dat diverse hogescholen (zoals de Noordelijke Hogeschool Leeuwarden, Hogeschool Zuyd, Fontys hogescholen, De Haagse Hogeschool en Saxion Hogeschool) bachelor- en masteropleidingen aanbieden op het terrein van veiligheid, informatiemanagement en ICT en recht met cybergerelateerde specialisaties. Veel van deze opleidingen zijn gepositioneerd in het informaticadomein.
Universiteiten , zoals de Universiteit Twente, Technische



Opleidingsconcept postinitiële master Cyber Security

Universiteit Delft, Radboud Universiteit Nijmegen, Vrije Universiteit en TU-Eindhoven bieden (al dan niet in combinatie met elkaar) technische tracks aan (zoals binnen het Kerckhoff's instituut), veelal als specialisatie van uiteenlopende opleidingen Computer Science. Andere universiteiten bieden tracks en masteropleidingen op het grensvlak van disciplines zoals Law and Technology (de Universiteit van Tilburg en de Universiteit Leiden) Forensics en inlichtingenstudies (Universiteit van Amsterdam) en Safety & Security (Universiteit Leiden) en Cyber and Business (Nyenrode Business University). De drie technische universiteiten hebben het initiatief genomen om in samenwerking met elkaar (mogelijk aangevuld met derden) een nieuwe (overwegend technische) master Cyber Security te ontwikkelen (beoogde start in 2015).
Naast het bachelor- en masteraanbod van universiteiten en hogescholen bieden tal van private bedrijven en organisaties gespecialiseerde korte cursussen, leergangen, workshops e.d. op het terrein van Cyber Security. Bekende aanbieders zijn Deloitte, FOX-IT , ENCS, Thales, VKA, KPMG, TNO, Security Academy e.a.
In Europees verband verdienen University College Dublin en diverse universiteiten in de UK vermelding (University of Warwick, Royal Halloway London, University of Oxford en Lancaster University). Ook eerste open online onderwijsvarianten (MOOC's) zijn in ontwikkeling (University of Maryland). Veel van deze opleidingen kennen een sterke focus op technische knowhow met een enkele keuzemogelijkheid in het domein Recht en/of Bestuurskunde.

De multidisciplinaire executive master Cyber Security

Nog vrijwel nergens blijken vraagstukken rond cyber security vanuit holistisch perspectief bestudeerd te worden. Mede in het verband van het beschikbare netwerk van bedrijven en instellingen verenigd in The Hague Security Delta deed zich voor kennisinstellingen voor hoger onderwijs in de Haagse regio de unieke gelegenheid voor om een multidisciplinair opleidingsconcept te ontwikkelen en aan te bieden.

In deze parttime eenjarige Engelstalige MSc opleiding (verspreid aangeboden over twee jaar) voor zowel technisch als juridisch en sociaal wetenschappelijk geschoolde deelnemers, wordt vanuit een gemeenschappelijk framework (introduction into cyber) in twee (verdiepende) specialisaties (technical en governance track) met behulp van uiteenlopende verbredende en verdiepende keuzemodules (variërend van o.a. cyber forensics, cyber espionage en tot cybercrime and law enforcement) en een individueel uit te voeren onderzoek (de masterthesis) toegewerkt naar een nieuw type cyber security-professional voor functies van de toekomst.

Referenties

[1] De opleiding is inmiddels door de Universiteit Leiden ter accreditatie voorgelegd aan de NVAO.

[2] http://www.internetworldstats.com/emarketing.htm

[3] Nationale Cyber Security Strategie 2, oktober 2013

[4] Prof. dr. Wouter Stol, prof. dr. Pieter Hartel en prof. dr. Jan van den Berg, e.a.