Verslag CSR (Mini-)Seminar 'Internet of Things'

Locatie: Nieuwe of Littéraire Sociëteit De Witte
Plein 24, 2511 CS Den Haag
Datum: dinsdag 21 november 2017
Aanvang: 17.00 – 21.30 uur

Op dinsdagavond 21 november jl. vond op initiatief van de Cyber Security Raad (CSR) een besloten (mini-)seminar met als thema 'Internet of Things' (IoT) plaats. Het programma startte om 17.00 uur en vond plaats in de Nieuwe of Littéraire Sociëteit De Witte in Den Haag. De genodigden voor deze avond waren CEO's, bestuurders en topmanagers uit de publieke, private én wetenschappelijke sector, waaronder afgevaardigden van ministeries, topbestuurders/-managers, wetenschappers, CEO's van bedrijven en instellingen, aantal studenten van de NCS3 en raadsleden van de CSR. Aanleiding voor het seminar was het afscheid van de heer drs. Eelco Blok als covoorzitter van de raad.

Dankwoord van de minister
Het seminar werd geopend door de minister van Justitie en Veiligheid, prof. mr. F.B.J. (Ferdinand) Grapperhaus. Hij bedankte de heer Eelco Blok persoonlijk voor zijn inzet als covoorzitter van de CSR in de afgelopen jaren. Sinds de oprichting van de raad in 2011 is Eelco Blok covoorzitter van de Raad geweest. En al die tijd heeft hij zich volop ingezet om cybersecurity op de agenda te krijgen. Niet alleen in boardroomgesprekken bij bedrijven, maar ook bij publieke optredens op congressen en bijeenkomsten. Het landsbelang stond voor hem daarbij altijd centraal. Grapperhaus: "Eelco heeft zich kwetsbaar opgesteld doordat hij na de grote hack bij KPN in 2012 zijn eigen ervaringen heeft durven te delen, zodat andere organisaties niet hetzelfde zou overkomen." Ook ging de minister in op een aantal belangrijke wapenfeiten die de CSR onder leiding van Eelco Blok in Nederland heeft bereikt.

De volledige speech van minister Grapperhaus is terug te lezen op het internet:
https://www.rijksoverheid.nl/documenten/toespraken/2017/11/21/toespraak-minister-grapperhaus-tijdens-het-seminar-%E2%80%9Cinternet-of-things%E2%80%9D-tevens-afscheid-eelco-blok-als-co-voorzitter-van-de-cyber-security-raad

Nanotechnologie
de heer prof. dr. ing. Dave Blank is nanotechnoloog en nanotech futurist. Hij verzorgde de eerste inleiding van het seminar. Dankzij nanotechnologie zijn we in staat materie op de schaal van individuele atomen en moleculen niet alleen te bestuderen, maar ook naar onze hand te zetten. Op deze schaal gaan de wetten van de quantummechanica een belangrijke rol spelen. Nieuwe toepassingen van quantum- en nanotechnologie kunnen en zullen de samenleving ingrijpend veranderen. Zo vertelt Dave Blank over een nanopil die o.a. darmkanker kan opsporen en op den duur een medicijn in het lichaam

los moet kunnen laten. Ook voorspelt hij dat in de toekomst een quantum computer wordt ontwikkeld die een miljoen keer beter is dan de beste computer van dit moment. Quantumcomputing geeft bovendien toegang tot ongekende rekenkrachten om de eigenschappen van materialen, chemische processen en geneesmiddelen te voorspellen en te verbeteren. Daarnaast presenteerde Blank de eerste resultaten van computers die gebaseerd zijn op de werking van de hersenen.
Nieuwe toepassingen van quantum- en nanotechnologie kunnen en zullen de samenleving ingrijpend veranderen. Daarbij is ook de aandacht voor cybersecurity van belang. In dit kader legde Blank twee stellingen ter discussie voor aan de genodigden:

Stellingen:

- Voor (cyber)security is het essentieel dat Nederland leidend blijft in de ontwikkeling van nieuwe technologieën, zoals nanotech.
- Er moet meer aandacht komen voor de effecten in cybersecurity bij het onderzoek naar nieuwe technologieën, zoals nanotech.

Belangrijkste conclusies :

- Een leidende positie van Nederland in cybersecurity wordt als noodzakelijk gezien.
- Nederland is een klein land, samenwerking met andere landen (allianties) is belangrijk om grote stappen te kunnen zetten.
- Nanotechnologie moet gestimuleerd worden, security en privacy by design zijn daarbij randvoorwaardelijk.
- Het is belangrijk om bij nanotechnologie aandacht te besteden aan de risicobeheersing en drempelverhoging van technologie alsook in hoeverre eventuele risico's vooraf zijn te reguleren.
- Investering in fundamenteel onderzoek is nodig en belangrijk. Een wisselwerking tussen verschillende onderzoeksdomeinen (cyber en technologie) is daarbij van belang, onder andere voor de security by design. Ook is er meer behoefte aan de vertaalslag van wetenschap naar praktijk.
- Nanotechnologie brengt ethische risico's met zich mee; voorlichting en regelgeving is van belang. De leverancier is en blijft verantwoordelijk en aansprakelijk voor de digitale veiligheid van zijn producten en diensten.
- Er moet gezocht worden naar synergie tussen sectoren waar Nederland een sterke positie heeft, bijvoorbeeld landbouw.
- Op de onderwerpen waar Nederland niet zelfstandig kan acteren, is het belangrijk dit op Europees niveau op te pakken.

eMobility
De tweede inleiding van de avond werd verzorgd door ir. Gilles Ampt CISM CIPP/E, voorzitter van de Security Community Smart Mobility. In de hele ontwikkeling naar volledig autonoom rijden, zie je dat de klassieke bestuurder steeds meer naar de achtergrond verdwijnt. De techniek neemt geleidelijk aan de voorheen menselijke reacties (op basis van oren en ogen) over. Het individuele voertuig wordt uiteindelijk via systemen met internet verbonden en dat schept nieuwe type risico's, denk daarbij aan diefstal van voertuigen, gegevensverlies, manipulatie van motormanagement en besturing en betrouwbaarheid van communicatieprocessen en informatieoverdracht. Nederland wil een voorsprong

nemen in eMobility voor meer efficiëntie in verkeer zodat we bijvoorbeeld files kunnen vermijden, automatisch ruimte op wegen kunnen maken voor zogeheten 'noodverkeer' als ambulances, groene golf verkeerslichten en meer. De focus ligt op het goed functioneren van het collectieve verkeerssysteem. Allerlei partijen in de auto-industrie garanderen de technische veiligheid van individuele voertuigen en voertuigtypes, maar hoe verhouden deze veilige voertuigen zich tot een gegarandeerde veiligheid van het collectieve verkeersysteem (denk aan (systemen van) de auto-industrie en de toezichthouder RDW)? Hoe voorkom je dat een gemanipuleerd voertuig ongewenste risico's veroorzaakt aan het collectief? Wie ziet hier op toe? Na afloop van de inleiding ging het in de discussie met de aanwezigen onder meer over de vergelijking met de luchtvaartindustrie. Die loopt mijlenver voor op het wegverkeerssysteem. Een boeiende vraag was, als de mens de zwakste schakel is in het verkeerssysteem, hoe wordt de automobilist straks, bij langdurige periodes van autonoom rijden, in staat gesteld de besturing van het voertuig weer over te nemen? Kan de automobilist dat nog wel als dat nodig is? Ook Ampt eindigde zijn bijdrage met twee stellingen voor de genodigden:

<u>Stellingen:</u>

- Toegang tot het internet en andere openbare communicatienetwerken voor apparaten dient gereguleerd te worden voor hun gehele economische levensduur. Voor elke sector is een eigen aanpak nodig.
- In de regulering van internettoegang voor apparaten dienen cybersecurity en dataprotectie (persoonsgegevens) integraal meegenomen te worden.

<u>Belangrijkste conclusies:</u>

- Regulering voor toegang tot het internet is niet wenselijk. Wel zijn minimum eisen voor security gewenst en handhaving hiervan.
- Security en privacy by design zijn randvoorwaardelijk.
- Meer aandacht voor awareness bij gebruikers: van onbewust/onbekwaam naar bewust/bekwaam.
- De gebruiker moet centraal staan en maatwerk per sector is daarbij nodig.
- Er moet ook aandacht zijn voor analoge fallback-scenario's.
- Er moet blijvend geanticipeerd worden op de toekomst.

Europese cyberstrategie

De laatste inleiding van de avond werd verzorgd door Dr. Paul Timmers, onafhankelijk adviseur voor digitale innovatie en voormalig directeur van de Europese Commissie voor Digital Society, Trust & Cybersecurity. Timmers is betrokken geweest bij de totstandkoming van de update van de Europese Cybersecurity strategie en de totstandkoming van onder andere de NIB-richtlijn, de eerste 'cybersecurity-wetgeving' op Europees niveau. Met als titel 'Cybersecurity - de slag en de oorlog' nam Timmers de deelnemers mee in de geschiedenis van cyberaanvallen. Het IoT is volgens Timmers een gigantische cybersecurity-uitdaging. Miljarden devices zijn aangesloten op het internet, waarvan 70% onbeschermd. Security is in conflict met lage kosten, geringe rekenkracht en de complexiteit van het IoT. Het risico op nieuwe cyberaanvallen groeit exponentieel. De update van de EU Cybersecurity strategie moet ervoor zorgen dat we binnen Europa een omslag maken van een reactieve naar een proactieve benadering. Niet alleen voor de Europese welvaart, maatschappij en waarden, maar ook voor het beschermen van de grondrechten en fundamentele vrijheden door bestaande en toekomstige

dreigingen te pareren. De update was noodzakelijk door onder andere alle nieuwe technologische ontwikkelingen, zoals het IoT. Bedrijven en burgers zijn nog even bezorgd en slecht voorbereid en er is een enorme groei van de economische impact van cyberincidenten.
Volgens Timmers gaan we de cyberslag verliezen en de cyberoorlog winnen. Op korte termijn zijn we aan de verliezende hand door de toename van de kwetsbaarheid van nieuwe technologie, zoals het IoT, het gebrek aan governance en brede samenwerking. Op de langere termijn stelt Timmers 'we will get our act together' en zien we technologie als partner, is er sprake van meer samenwerking en is 'cyber in alle policies'. Zijn de genodigden van de avond het met hem eens? Timmers daagde de deelnemers uit een scenario te kiezen.

Stelling:
Cyber-oorlog versus cyberslag: winnen of verliezen? Kies een scenario:

Conclusies:
Op een enkele uitzondering na (verlies-win), kozen de meeste genodigden voor het 'win-win-scenario'. Belangrijkste argumenten en aandachtspunten die daarbij zijn genoemd:

- Cyber-oorlog versus cyberslag is een permanente ratrace. Alle scenario's zijn een momentopname. Het cyberlandschap is continu in beweging en hierop dienen we altijd voorbereid te zijn.
- Denken in termen van oorlog is belangrijk om op langere termijn de strijd te winnen. Digitaal leiderschap is daarbij nodig.
- Je kunt de oorlog winnen door bewust een slag te verliezen.
- Crowed wisdom: ontwikkelingen gaan zo snel dat je meer profijt hebt om kennis en informatie te delen in verhouding tot het risico van diefstal van kennis en informatie.
- We moeten voorop blijven lopen ten opzichte van de concurrentie in de EU om te kunnen winnen. Dit trekt ook talent.
- Het is belangrijk gecalculeerd je verlies te pakken (you win some, you lose some); geen risico's nemen in de vitale sectoren.
- Wil je de slag niet verliezen dan moet je georganiseerde tegenspraak organiseren. Wetenschappelijke inzichten moeten worden gebruikt voor de operatie. De operatie loopt per definitie achter. De verbinding tussen operatie en wetenschap moet worden gezocht. Dit gebeurt al veelvuldig in de medische wereld.
- Wees altijd voorbereid op eventuele permanente disruptie (fallback-scenario's).
- Voorkom vertrouwensbreuk met de burger.
- Er moet meer aandacht komen voor (verplichte) security awarenesstrainingen en meer nadruk komen op open-source aanpak.
- 'This is not a *policy* war but a *tech* war': met andere woorden we hebben vooral meer technische specialisten nodig om de oorlog te kunnen winnen.

Afsluiting

Na de terugkoppeling van de uitkomsten van de laatste discussie was het woord aan de heer drs. Eelco Blok. Aan hem de eer om het seminar af te sluiten. Volgens Blok kunnen we terugkijken op een zeer geslaagde avond met een mooie opbrengst aan conclusies die de CSR verder op kan pakken. Blok maakte van deze gelegenheid ook gebruik om een aantal personen te bedanken. Zijn eerste dankwoord ging naar de heer drs. Dick Schoof met wie Eelco de laatste vier jaar gezamenlijk het covoorzittersschap van de raad vervulde. Ook dankte hij Elly van den Heuvel, secretaris van de CSR, voor haar belangrijke bijdrage aan de ontwikkeling van de raad en haar ondersteuning in de afgelopen jaren voor hem als covoorzitter alsook voor de organisatie van deze avond. Een dankwoord was er ook voor alle aanwezigen van de avond voor hun komst en hun bijdrage.