

Jaarcongres 2009

Hup Holland Hub



KIVI NIRIA

Workshop Cyberverdediging

Nederland speelt met zijn ICT rotonde wereldwijd in de championsleague. Cyberspace is een hele aparte dimensie van ons leven geworden. Maar weten we voldoende hoe we onze cyberspace moeten verdedigen en doen we dat adequaat? We hebben namelijk nogal wat te verdedigen. Denk daarbij niet alleen aan openbare veiligheid, transport en de financiële wereld, maar bijvoorbeeld ook aan onze drinkwater-, energie- en voedselvoorziening. Wat ligt er zoal op de loer aan gevaren binnen onze cyberspace. Allereerst de betrekkelijk 'onschuldige' zaken als natuurgeweld, falen van de techniek en falen door menselijk handelen. Een hogere schaal ellende wordt in oplopende dreiging veroorzaakt door funhackers, criminelen, activisten en terroristen. Zo levert hacken het criminele circuit jaarlijks 100 miljoen euro op, een lucratieve bezigheid dus. Inmiddels waarschuwt het Britse MI5 bedrijven om goed te waken over hun cyberbeveiliging. Van een cyberoorlog is in de wereld nog geen sprake, maar wel zijn de eerste aanvallen bekend.

In Nederland is de keten van cyberbeveiliging niet gesloten, er is te veel verzuiling en te weinig samenwerking. Zo is er een telecomwet voor telefonie, Wet computercriminaliteit voor internet en de Wet bescherming persoonsgegevens, die niet consistent zijn juist waar dat zo nodig is. Ook is de verantwoordelijkheid van onze cyberspace verdeeld over verschillende ministeries wat een geïntegreerde aanpak niet bevordert. Op dit moment is de aanval de beste verdediging: Nederland moet zich voorbereiden op alle mogelijke aanvallen en dit ook oefenen. Daarnaast is onderzoek nodig en zijn bijvoorbeeld trendanalyses noodzakelijk.

Het Ministerie van Algemene Zaken zou de regie moeten voeren over de beveiliging van onze cyberspace juist omdat cyberbeveiliging door alle lagen heen gaat. De ontwikkeling van een cyber security strategie is van het grootste belang en verdient grote prioriteit.