Digitale Binnenhof Academy

8 april 2021

Digitale Binnenhof Academy – Outline lezing Digitale Veiligheid

De openingslezing van de Digitale Binnenhof Academy ging over het thema '**digitale veiligheid**'. De lezing is gegeven door **prof.dr. Bibi van den Berg**, als Hoogleraar Cybersecurity Governance verbonden aan de Universiteit Leiden en tevens één van de vier wetenschappelijke leden van de Cybersecurity Raad, de raad die het kabinet gevraagd en ongevraagd advies geeft op het terrein van digitale veiligheid.

Van den Berg is in haar 45 minuten durende lezing ingaan op de volgende zaken:

1. **Wat is digitale veiligheid?**
   Digitale veiligheid is een groot domein, dat veel verschillende typen dreigingen omvat. Hoe kun je dat grote domein beter begrijpen? Aan de hand van twee modellen werd voor deelnemers inzichtelijk gemaakt waar discussies rondom digitale veiligheid over gaan:
   - Het **cyber harm model** (Van den Berg & Kuipers, 2021) laat zien dat incidenten kunnen leiden tot schade *in* cyberspace (data wordt gestolen, een systeem wordt gehackt), maar ook tot schade *via* cyberspace (een dam wordt gehackt en daardoor wordt een deel van Nederland onder water gezet). Dit kanaliseert het gesprek over de (on)tastbaarheid van de consequenties van incidenten. Hetzelfde model laat ook zien dat overheid, bedrijven en wetenschap vooralsnog primair gericht zijn op het adresseren van *intentionele dreigingen* (alles van een hack en een datalek tot sabotage en oorlogshandelingen, maar ook desinformatie en fake news), maar dat er (zorgwekkend genoeg) veel minder aandacht is voor *niet-intentionele dreigingen* (denk aan storingen, uitval en menselijke fouten). Het model fungeert als een 'praatplaat' waarmee politici alle grote uitdagingen uit het digitale veiligheidsdomein in één overzicht gekaderd krijgen. Zo komen ze beter beslagen ten ijs in discussies over deelonderwerpen binnen dit grote domein.
   - Het **prevent-detect-respond-governance model** (Van den Berg & Oldengarm, forthcoming) laat zien dat in de huidige realiteit organisaties èn overheden primair gericht zijn op het *voorkomen* van incidenten, veelal door gebruik te maken van risico management. Hoewel dit een belangrijke aanpak is en blijft, is in de afgelopen jaren ook gebleken dat incidenten, alle inzet ten spijt, toch zullen voorkomen (denk voor het publieke domein alleen al aan de Universiteit Maastricht (2019), de vele incidenten bij de GGD in 2020 en de gemeenten Lochem (2015) en Hof van Twente (2020)). Organisaties èn overheden doen er daarom goed aan hun focus te verleggen van uitsluitend voorkomen naar *detectie* van *incidenten* (gemiddeld duurt het 56 dagen voor een hack ontdekt wordt!) en *response* op incidenten. Voor politici is het belangrijk om te begrijpen (1) dat incidenten niet (altijd) voorkomen kunnen worden, en (2) dat het dus in de komende jaren belangrijker wordt te werken aan 'preparedness': wat moet een organisatie/een land doen ten tijde van een cybercrisis?

2. **Wat zijn de grootste uitdagingen voor de komende 4 jaar?**
   Welke uitdagingen zijn er voor Nederland in de komende 4 jaar (en daarna)?
   - **Digitale soevereiniteit**: één van de grootste zorgen in politiek Den Haag van dit moment betreft de vraag hoe om te gaan met onze internationale *afhankelijkheid* als het aankomt op digitale netwerktechnologie, zowel van grote internationale bedrijven (de discussie rondom de Big Five), alsook van andere mogendheden (China en 5g). Kan en moet Nederland manieren vinden om 'digitaal soeverein' te worden, en zo ja, hoe dan?

- **Weerbaarheid**: alle systemen die we gebruiken zijn intussen verbonden met cyberspace, met alle risico's van dien. Hoe waken we over onze *vitale infrastructuur* (en wat betekent het onderscheid 'vitaal/niet-vitaal' eigenlijk nog als alles en iedereen met elkaar verbonden is en van elkaar afhankelijk is? Wat kunnen we doen om te zorgen voor meer weerbaarheid?
- **Criminaliteit**: steeds meer criminaliteit verplaatst zich naar cyberspace, en de verwevenheid tussen online en offline criminaliteit neemt steeds verder toe. Hoe adresseren we dit (grensoverschrijdende) probleem?
- **Regie**: Wie *beheert* het 'dossier digitale veiligheid' in Nederland? Dat dossier is in handen van verschillende ministeries, die elk hun eigen taken en mandaten hebben. Daardoor is het beleidslandschap versnippert, zijn er uitdagingen waarop ministeries elkaar (onbedoeld) tegenwerken, en uitdagingen waar 'niemand van is'. Is het tijd voor een meer geïntegreerde aanpak van het thema cybersecurity? En wat is daar dan voor nodig?