19 september 2019

Geachte leden van de TCDT,

De vragen in uw uitnodigingsbrief luiden:

1. Welke thema’s op het terrein van digitalisering vragen aandacht van de Kamer in de nabije toekomst en waarom.
2. Op welke wijze zou de Kamer de grip op deze ontwikkelingen kunnen vergroten.

Deze komen overeen met vraag 1 en 3 in het TCDT-onderzoeksplan:

1. Welke bovenliggende thema’s op het terrein van digitalisering – zowel voor wat betreft technologische ontwikkelingen als maatschappelijke en economische impact - vragen aandacht van de Kamer in de nabije toekomst en waarom?
2. Wat is er – zowel inhoudelijk als institutioneel - nodig om de kennispositie van de Kamer ten aanzien van en grip op digitale ontwikkelingen te vergroten?

Mijn achtergrond ligt bij de politie en in de sociale wetenschappen (sociologie, criminologie). Sinds me­dio jaren tachtig van de vorige eeuw houd ik me bezig met onderzoek naar politie, veiligheid en nieuwe technologie. Sinds ongeveer 2007 richt mijn onderzoek zich op ‘cybersafety’: bescherming van mens en organisatie tegen onveiligheid die voortkomt uit het digitale domein. Mijn aandacht gaat speciaal uit naar de ‘human factor’ van digitale veiligheidsvraagstukken: daderschap, slacht­of­fer­­schap, opsporing, handhaving, rechtswaarborgen, verantwoordelijkheden, weerbaarheid, be­voegd­heden, organisatie, samen­wer­king – om enkele daarmee verbonden thema’s te noemen. Momen­teel ben ik lector Cybersafety aan NHL Stenden Hogeschool en aan de Politieacademie en bij­zon­der hoogleraar politiestudies aan de Open Universiteit.

Graag deel ik naar aanleiding van bovenstaande vragen enkele overwegingen met u.

Veiligheid is een basisvoorwaarde voor een goed functionerende samenleving. Ook voor digitale ont­wikkelingen geldt dus dat de zorg voor veiligheid prioriteit verdient. Het is mooi wat bijvoorbeeld robots, AI en quantumcomputing kunnen betekenen, maar als de introductie van een nieuwe tech­nologie nieuwe onveiligheden met zich mee brengt, is dat meteen een punt van zorg, vooral omdat de consequenties er van verreikend kunnen zijn. Ook hier is voorkómen beter dan genezen. Zorg voor een deugdelijke cybersecurity verdient dus bij alle ontwikkelingen van meet af aan aan­dacht. Het is een risico om zonder die aandacht te investeren in nieuwe ontwikkelingen.

‘Cybersecurity’ is van oudsher een begrip met een exclusief technologische lading, en soms nog steeds. Dat is ten onrechte. Zoals vaak, is ook in digitale veiligheid de mens de zwakke schakel. Uit­eindelijk is immers ook een slechte technologie een menselijk product, met menselijke gebruikers en menselijke belanghebbenden. Digitale veiligheid vergt dat technici en sociaal-wetenschappers van diverse pluimage de handen ineen slaan om in interdisciplinair verband te werken aan een digitaal veilige omgeving. Bij systeemontwikkeling, onderzoek naar nieuwe technologieën of het evalueren van bestaande technologieën is aandacht daarvoor gevraagd, maar ook bij onderwijs (bestaande en nieuwe opleidingen) en bij onder­zoek, zoals bij de verdeling van NWO-gelden.

Het onderwijs op het gebied van digitalisering en veiligheid is een thema dat aandacht verdient. De De dcypher[[1]](#footnote-1) adviesraad heeft naast het cybersecurity onderzoek ook het cybersecurity onderwijs als aandachtspunt en spant zich in om tot overzicht en afstemming te komen: afstemming tussen vraag en aanbod en afstemming tussen onderwijsinstellingen die mensen opleiden. Het ontwikkelen van onderwijs met betrekking tot digitalisering is een groeimarkt. Om voldoende deskundigheid in huis te hebben en te houden, lijkt het goed om te zorgen voor afstem­ming in het onderwijsaanbod en voor samenwerking tussen de verschillende onderwijsinstellingen – ook hier met het oog op een interdisciplinaire benadering. Specialisten zijn een noodzakelijk maar niet voldoende antwoord op de digitale vraagstukken.

Bij digitalisering is de aandacht al gauw gericht op bepaalde organisaties of functies, zoals ‘digitali­se­ring bij de politie’ of ‘digitalisering van gemalen’. Dat is begrijpelijk want dat goed te doen is al lastig genoeg. Aandacht verdient desondanks ook de wat bredere samenhang: ‘digitalisering van de straf­rechtketen’ of ‘digitalisering van het waterbeheer’ – om te voorkomen dat digitale eilandjes ont­staan met problemen op het gebied van informatieoverdracht, veiligheid en afstemming (samen­wer­king).

Overheidsorganisaties hebben een speciale verantwoordelijkheid aangaande digitalisering. Meer nog dan alle andere organisaties dienen zij hun digitale veiligheid en hun informatiebeveiliging goed op orde te hebben. Ze hebben een voorbeeldfunctie en ze hebben veel en gevoelige gegevens onder zich. Dat vergt goede beveiliging en effectieve noodprocedures (w.o. noodstroom, back-ups). Verder dienen overheidsorganisaties in de uitvoering van hun overheidstaken de stap naar digitalisering te zetten. In mijn werk bijvoor­beeld hield ik me tot 2014 uitsluitend bezig met digitalisering bij politie en OM. In 2014 startte ik de discussie wat gemeenten doen aan het bevorderen van de digitale veiligheid. Dat leefde toen hoegenaamd niet en nog steeds staan gemeenten voor een stevige inhaalslag, terwijl veiligheid één van hun kerntaken is. Het lijkt dus zaak om eens te inventariseren of alle overheids- en semi-overheidsorganisaties inmiddels werken aan het vertalen van hun kerntaken naar bemoeienis in het digitale domein. Het laat zich immers moeilijk voorstellen dat de gemeenten de laatsten zijn en alle andere overheids- en semi-overheidsorganisaties die slag al hebben gemaakt. Dit moet voorkomen dat ineens blijkt dat een deel van de (semi)overheid niet is meegekomen.

Zinvol nadenken over de toekomstige (digitale) vorm van oude functies, rollen of mogelijkheden, is niet altijd eenvoudig. Als je niet ver genoeg vooruitdenkt, kom je niet in de positie om te anticiperen. Eventuele actie komt dan te laat. Denk je wel ver vooruit, dan is het toekomstbeeld al gauw ‘ver ge­zocht’, wat wel leidt tot vrolijkheid maar niet tot anticiperende actie. Op strafrechtgebied is de (nog maar nauwelijks gevoerde) discussie over aanranding in een virtual reality game een voorbeeld. Kan een slachtoffer daarvan aangifte doen of moet de ‘iemand’ in ‘iemand [dwingen] tot het plegen of dulden van on­tuchtige handelingen’ (art 246 Sr) een fysiek iemand zijn? Is een wetswijziging wense­lijk? Als virtuele aanranding mogelijk wordt, dan ook virtuele mishandeling of moord? Wensen we dat? Vergt dat aanpassingen in de wetgeving? Dit soort handelingen eenvoudig onmogelijik maken is zelden een oplossing. Zoals één van mijn studenten in deze discussie zei: ‘je kan toch overal dingen kopen die je kan misbruiken, zoals een mes’. Een ander voorbeeld is de bevoegdheid van de politie tot het stelselmatig inwinnen van informatie (art. 126j Sv). Te voorzien valt dat dit gaat overlappen met de bevoegdheid tot onderzoek aan of in het lichaam (art. 56 Sv) nu het inwinnen van informatie ook betrekking kan hebben op gegevens uit iemands *smart watch* (lichaamstemperatuur, hartslag, beweging, transpiratie). Het eerste bovenliggende thema is de modernisering van ons straf(pro­ces)­recht. Over opsporingsbevoegdhden in een digitale heeft de commissie Koops (2018) belangwekkende dingen geschreven. De vraag is echter of we ook voor het overige (materieel recht) voldoende vooruit kijken. Het tweede bovenliggende thema is de vraag of (overheids)organisaties wel voldoende vooruit kijken, zodat zij voorbereid kunnen zijn op de ontwikkelingen.

Fabrikanten van ICT en aanbieders van digitale diensten beschikken vaak over veel informatie over gebruikers, die deze, zich al dan niet daarvan bewust, zelf verstrekken. Wat deze bedrijven doen met deze gegevens is een punt van aandacht. Verder zien we dat overheid en particuliere bedrijven die over veel gegevens beschikken, vaak samenwerken. Ook in de opsporing is dat het geval. Wanneer de overheid die gegevens gebruikt is de cruciale vraag of dat gebruik in overeenstemming is met grondrechten en rechtswaarborgen, of eigenlijk: of die gegevens ooit zijn verzameld met inachtneming van de zogvuldigheidseisen die zouden gelden wanneer de overheid die gegevens had verzameld. Publiek-private samenwerking is als het om het uitwisselen van gegevens gaat een onderwerp dat regulering behoeft.

Dat brengt me bij de tweede vraag.

Het samenlevingsbreed sturen van technologsiche ontwikkelingen is geen sinecure. Maar onmogelijk is het niet. Ik gebruik hier graag het voorbeeld van het aantal verkeersdoden in Nederland. Dat steeg vanaf de jaren ’50 dramatisch naar meer dan 3.000 begin jaren ‘70. Daarna zette de daling in tot ongeveer 600 in 2010 (ondanks het gestegen aantal reizigerskilometers). Recent zagen we weer een stijging vanwege nieuwe ontwikkelingen (bv. vergrijzing, elektrische fiets). Hieruit mogen we leren dat (a) het is mogelijk om ongewenste neveneffecten van een nieuwe, massaal gebruikte technologie (i.c. m.n. de auto) te reduceren, (b) dat vergt tientallen jaren en (c) de inzet van een grote diversiteit aan maatregelen (i.c. bv. gordelplicht, helmplicht, verbod op rijden zonder invloed, bouwen aan veilige weginfrastructuur, veiliger auto’s, APK, educatie, handhaving, en cultuurverandering). Bijsturen van ongewenste effecten van technologsiche ontwikkelingen vergt: (i) een indicator van het probleem (i.c. aantal verkeersslachtoffers), (ii) het daarmee monitoren van de omvang van het probleem (onderzoek, statistiek), (iii) een lange termijn visie en dus lange adem (decennia), (iv) een brede mix van maatregelen, (v) evaluatieonderzoek m.b.t. de effectiviteit van maatregelen, (vi) kennis om dit alles uit te voeren (onderwijs).

Cruciaal is is vinden van een breed gedragen indicator die de omvang van het probleem op hoofdlijnen aangeeft. Het aantal verkeersslachtoffers is een schoolvoorbeeld. Om de negatieve gevolgen van digitalisering in kaart te brengen valt bijvoorbeeld te denken aan het aantal geslaagde hacks, het aantal datalekken, veiligheidsgevoelens in een digitale omgeving. Het is zaak om een set van indicatoren vast te stellen waarmee we ons kunnen voorzien van een beeld van de schaduwkant van de digitalisering.

Verder is bij het sturen van technologische ontwikkelingen van belang om er snel bij te zijn. Dat is ten aanzien van de digitalisering als geheel denk ik niet gelukt maar wellicht kan dat nog wel op nieuwe ontwikkelingen binnen de digitalisering als geheel. Wat die nieuwe ontwikkelingen zijn, is te achterhalen door daarover te spreken met experts uit verschillende richtingen. Op deelgebieden gebeurt dat ook wel in de vorm van trendonderzoek.

Ook binnen (overheids)organisaties kan sturing gegeven worden aan de digitale weerbaarheid van de organisatie en haar cybersecurity. De ervaringen bij de politie hebben laten zien dat dat niet gaat zonder specialisten of voortrekkers. Tegelijk is de aanwezigheid van specialisten niet genoeg want alle werknemers van een organisatie zullen moeten meebewegen met de digitalisering om hun taken goed te blijven doen en zullen ook hun aandeel moeten hebben in digitale veiligheid. Binnen organisaties is dus een combinatie vereist van specialisten en een brede ontwikkeling onder alle werknemers. Een thema dat zich hieruit aandient is het helpen van (overheids)organisaties bij het doormaken van deze ontwikkeling.

Tot slot wens ik u veel succes met uw werk op de weg die we als samenleving gaan in het beheersen van de ongewenste gevolgen van digitalisering.

Met vriendelijke groet,

Wouter Stol.

1. Dutch Cyber Security Platform Higher Education and Research, [www.dcypher.nl](http://www.dcypher.nl), een platform mogelijk gemaakt door vier ministeries en NWO. [↑](#footnote-ref-1)