Toekomst-verkenning: *Het cyberdomein in 2022*

Analistennetwerk Nationale Veiligheid

Toekomstverkenning: Het cyberdomein in 2022

Analistennetwerk Nationale Veiligheid

Allard Kernkamp (TNO)
Sico van der Meer (Instituut Clingendael)
Eric Luiijf (TNO)
Maarten Gehem (HCSS)
Douwe Bierma (TNO)
Marcel Mennen (RIVM, editor)

Colofon

De Toekomstverkenning: Het cyberdomein in 2022 is gemaakt door het Analistennetwerk Nationale Veiligheid in opdracht van de NCTV, directie Cybersecurity van het ministerie van Veiligheid en Justitie

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
van het ministerie van Veiligheid en Justitie
De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
De Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO
De Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael'
Het Institute of Social Studies (ISS) van de Erasmus Universiteit Rotterdam

Allard Kernkamp (TNO)
Sico van der Meer (Instituut Clingendael)
Eric Luiijf (TNO)
Maarten Gehem (HCSS)

Contact: douwe.bierma@tno.nl

Inhoud

Opdracht en doelstelling

De opdracht

De NCTV, directie Cybersecurity van het ministerie van Veiligheid en Justitie heeft het Analistennetwerk Nationale Veiligheid opdracht gegeven een aantal cyber-toekomstscenario's op te stellen die zich afspelen rond 2022. Deze scenario analyse heeft tot doel de ontwikkeling van een geïntegreerd inter-departementaal beleid in het digitale domein te ondersteunen.

Het Analistennetwerk Nationale Veiligheid

Het Analistennetwerk Nationale Veiligheid (ANV) is een gezaghebbend kennisnetwerk dat sinds 2011 in opdracht van het ministerie van Veiligheid en Justitie, namens de Stuurgroep Nationale Veiligheid (SNV), onafhankelijk scenario analyses verricht ten behoeve van het Nationaal Veiligheidsprofiel (NVP), voorheen de Nationale Risicobeoordeling (NRB). Daarnaast voert het ANV andere (ad hoc) analyses en studies uit van mogelijke bedreigingen of de toekomst van onze nationale veiligheid.
Het ANV (zie Bijlage 1 voor een korte beschrijving) bestaat uit een vaste kern van zes organisaties en een omvangrijk netwerk van kennisinstellingen, uitvoeringsdiensten, bedrijven en adviesbureaus die afhankelijk van de kennisvraag worden ingeschakeld bij de te leveren producten. De vaste kern wordt gevormd door het RIVM, de AIVD, TNO, het instituut Clingendael, het WODC en het Institute of Social Studies van de Erasmus Universiteit Rotterdam (ISS). Deze instellingen dragen gezamenlijk de verant-woordelijkheid voor de inhoudelijke kwaliteit van het NVP en de andere producten van het netwerk.

TNO en schrijversteam

De uitvoering van deze opdracht is gecoördineerd en begeleid door TNO, partner in het ANV. TNO heeft het plan van aanpak opgesteld en afgestemd met de opdrachtgever, het proces gecoördineerd en de methodische begeleiding en borging verzorgd. De scenario's zijn geschreven door een groep bestaande uit vertegenwoordigers van HCSS, Instituut Clingendael en TNO.

Het rapport

Dit rapport beschrijft vier toekomstscenario's omtrent het cyberdomein in 2022, en hoe dit de positie van Nederland beïnvloedt. De vier scenario's zijn zo gekozen dat zij verschillende vormen van machtsverhoudingen, conflictsituaties, internet governance en technologieadoptie omvatten. Daarmee belichten zij de onderwerpen economie, privacy/vrijheid en veiligheid elk op een eigen wijze.

1 Inleiding

Voor u ligt de toekomstverkenning "Toekomstscenario's in het cyberdomein". De NCTV, directie Cybersecurity van het ministerie van Veiligheid en Justitie heeft het Analistennetwerk Nationale Veiligheid (ANV) opdracht gegeven een aantal cyber toekomstscenario's op te stellen die zich afspelen rond 2022.
De uitvoering van deze opdracht is gecoördineerd en begeleid door TNO, partner in het ANV. het proces gecoördineerd en de methodische begeleiding en borging verzorgd.
TNO heeft een Plan van Aanpak en een methodiek voorgesteld en beide afgestemd met de opdrachtgever en een klankbordgroep, bestaande uit vertegenwoordigers van het Ministerie van Defensie, het Ministerie van Ven J (NCTV/DCS en NCTV/DAS), het Ministerie van EZ en het Ministerie van BuZa.

De hoofdvraag

De hoofdvraag van het Ministerie van Veiligheid en Justitie luidde als volgt:
Op welke wijze kunnen als gevolg van welke ontwikkelingen economische groei, veiligheid en vrijheid in het digitale domein, zich (bij gelijkblijvend beleid) in en voor Nederland manifesteren in 2020?

De scenario's dienen bijzondere aandacht te geven aan de specifiek Nederlandse situatie ten aanzien van wet- en regelgeving, het hoge internetgebruik en snelle adoptie van nieuwe technologieën in de Nederlandse maatschappij en bedrijfsleven en de internationale Nederlandse positie als internetknooppunt en voorvechter van digitale vrijheid. De scenario's bevatten de volgende thema's :

- *Global commercial power en staatsmacht in het digitale domein*
- *Internet*[1] *governance*
- *Cyberconflict*
- *Ontwikkeling en adoptie nieuwe technologieën*

[1] In de Nationale Cyber Security Strategie wordt de term cyberspace gebruikt in plaats van internet, dat deel uit maakt van cyberspace en dus beperkter is. In dit opdrachtverlening is uitgegaan van het begrip Internet governance en daarom wordt deze term hier gebruikt. In de scenario's komen beide termen voor.

Plan van Aanpak

Omdat het Ministerie van Ven J had verzocht de scenario's in een kort tijdsbestek op te leveren, is er gekozen voor een beproefde werkwijze die een snel resultaat oplevert. TNO heeft de TNO Challenge ontwikkeld en beproefd voor vragen die een snelle oplossingen behoeven. TNO heeft deze werkwijze voorgesteld om te gebruiken om de gevraagde opleverdatum te kunnen behalen.

De voorgestelde werkwijze om tot de gevraagde scenario's te komen bestaat uit twee stappen:

1. **Brainstorm bijeenkomst**. Een aantal experts met verschillende achtergronden delen hun toekomstbeelden en trends met de schrijver in een kleine groep (6 tot 8 personen).

Op 4 september hebben genodigden van de volgende organisaties deelgenomen aan de brainstorm bijeenkomst: Instituut Clingendael, Defensie Academie, SIDN Fonds, Universiteit Leiden, TU Delft, Centric, Haagse Hogeschool, WRR, Rathenau, HCSS, Fox-IT, Radboud Universiteit, Tektok, NCSC, Centraal Plan Bureau, Schuberg Phillis en Radically Open Security. De scenarioschrijvers hebben op een directe en een indirecte wijze informatie tot zich genomen. Door vier groepen te creëren van zeven à acht personen zijn aan de hand van verschillende vragen discussies gehouden over toekomstige ontwikkelingen. Iedere schrijver heeft direct deze informatie tot zich genomen. Na afloop van de groepsdiscussie zijn de kernpunten in iedere discussiegroep plenair samengevat en besproken (indirecte informatieoverdracht). Een overzicht hiervan is weergegeven in Bijlage 3. Daarin is ook een lijst met de deelnemers aan de sessie opgenomen.

2. **TNO Challenge**. In één week tijd werkt het team van vier schrijvers het scenariostelsel, de scenario's én de eerste effecten op economie, privacy/vrijheid en veiligheid uit. Aan het eind van de Challenge week worden de scenario's opgeleverd en gepresenteerd aan het Ministerie van VenJ.

Het schrijversteam bestaat uit medewerkers van Instituut Clingendael, HCSS en TNO.

Methodiek

De voor deze opdracht uitgewerkte methodiek, in casu het voor dit doel uitgewerkte scenariostelsel dat is gebruikt als basis voor de TNO Challenge, staat beschreven in Bijlage 2.

Schrijversteam

Het schrijversteam bestaat uit:
Allard Kernkamp (TNO)
Sico van der Meer (Instituut Clingendael)
Eric Luiijf (TNO)
Maarten Gehem (HCSS)

Samenvatting scenario's en leeswijzer

In de "Challenge Week" zijn de volgende vier toekomstscenario's ontwikkeld.

- **Block Power**
  In dit scenario is sprake van verschuivende machtsverhoudingen op verschillende terreinen zoals enonomie, politiek en militair. Daarnaast is er sprake van maatschappelijke spanning tussen burgers en tussen burgers en overheid. De zelf- en samenredzaamheid van burgers staat onder spanning. Er wordt gezocht naar nieuwe verbindingen.

- **Bit Bang**
  Door een cyberaanval op de registratiesystemen wordt de samenleving als in een "slow cooker" langzaam maar zeker meer en meer ontwricht. De overheid verliest grip op de samenleving, individuen verliezen hun identiteit en daarmee kansen in de samenleving. Het is onduidelijk waar de aanval vandaan is gekomen. Er zijn verschillende cyber-koninkrijkjes die elk hun eigen positieve of negatieve invloed hebben op de samenleving.

- **Splitting Society**
  De samenleving is hyperconnected. Alles en iedereen is wereldwijd met elkaar verbonden. Er is een grote groei in een nieuwe high tech industrie, maar vooral voor diegenen die daar baat bij hebben. Een grote groep van digibeten kan de vergaande digitalisering niet meer aan. Educatie heeft niet genoeg aandacht gekregen. Er ontstaan diverse protestbewegingen. Er is een wankel evenwicht tussen veiligheid en onveiligheid.

- **Safe Haven**
  Door een cyberaanval is er een toenemende vraag naar standaarden om individuen en collectieven te beveiligen. Vanwege de standaardisatie verloopt de technologische innovatie langzaam. Er komen handels-vrijplaatsen voor producten en diensten die niet gestandaardiseerd zijn, maar wel veel mogelijkheden ten goede en ten kwade bieden. Door de standaardisatie komt er vertrouwen in zowel producten en diensten als in de overheid.

De scenario's zijn beschreven in de opeenvolgende hoofdstukken 2 tot en met 5.
Per scenario wordt er in separate paragrafen aandacht besteed aan de onderwerpen
- Staatsmacht
- Cyber conflict
- Internet Governance
- Adoptie van technologie

Tevens worden de scenario's bezien op effecten op de volgende drie terreinen:
- Economie
- Vrijheid / privacy
- Veiligheid

Tot slot worden de scenario's afgesloten met enkele conclusies in de vorm van mogelijke dilemma's, te betrekken stakeholders en kansen.

2 Scenario Block Power

2.1 Samenvatting

In 2022 is de wereld verdeeld in machtsblokken. Nederland hoort bij het door de VS gedomineerde Vrijheidskamp, waar het binnen de Europese landen een leidende rol op zich neemt als hoeder van onze privacy. China, Rusland en een aantal andere autoritaire landen hebben zich aaneengesloten in het Harmonieblok, met sterke overheidscensuur en repressie van 'staatsondermijnende' hackers. Cyberaanvallen, en met name staatsgedreven cyberspionage tussen de blokken, nemen sterk toe. Die aanvallen lijken vooral uit China en Rusland te komen, maar tegelijkertijd blijft de angst bestaan dat ook coalitiegenoten ons op grote schaal bespieden. Hoewel de wereldhandel afgelopen jaren is gekelderd, heeft Nederland zich als een van de eerste landen uit de economische malaise weten te ontworstelen, mede dankzij een florerend 'cyber-cluster', dat onder andere *world leading* encryptie-technieken voortbracht. Tegelijkertijd tekenen zich binnen de Nederlandse samenleving nieuwe spanningen af door binnenlandse economische verschuivingen en bewegingen die pleiten voor een sterkere focus op veiligheid, of juist aansluiting bij het Harmoniekamp.

2.2 Wat ging eraan vooraf

Vlak voor de Amerikaanse Presidentsverkiezingen in 2016 komt aan het licht dat de ICT van overheids-diensten in de VS grootschalig zijn geïnfiltreerd. Jarenlang werd al het diplomatieke verkeer, gerubri-ceerde documenten en privécorrespondentie van ambtenaren afgetapt. Wanneer blijkt dat de datastromen te herleiden zijn tot Chinese en Russische computers, ontstaan op verschillende plekken in de VS protesten, waarbij Chinese en Russische vlaggen worden verbrand. Producten uit China en Rusland worden geboycot, en in een aantal *Chinatowns* van grote Amerikaanse steden breken (weliswaar kleinschalige) rellen uit. Hoewel de Chinese en Russische overheid ontkennen iets met de infiltraties te maken te hebben, draait de Presidentsverkiezing uit op een klaterende overwin-ning voor een conservatieve kandidaat, die met zijn anti-China en -Rusland retoriek meer dan 60% van de stemmen binnenhaalt.
De spanningen nemen verder toe wanneer de Russen het jaar daarop e-mails vrijgeven die de complottheorie zou bevestigen dat de Republikeinen zélf achter de aanvallen zitten. Aanvankelijk probeert Nederland samen met andere EU-landen te mediëren tussen de supermachten. Maar dat verandert wanneer blijkt dat ook de Nederlandse overheid jarenlang werd afgetapt door – vermoedelijk – de

Chinese en Russische geheime diensten. Wanneer een Chinees bedrijf met een obscuur databeleid in Nederland gratis internet wil aanbieden, breken ook hier demonstraties uit en wordt de roep groter om kleur te bekennen en ons te voegen bij wat de Amerikanen *The Free World* ('het Vrijheidsblok') noemen. Die keuze volgt na een polariserend debat – en hevige Amerikaanse druk achter de schermen. En die keuze blijft niet zonder economische gevolgen: evenals andere westerse landen kampt de Nederlandse economie al jaren met flinke krimp. De afzetmarkt voor onze export keldert, omdat de toegang tot Chinese en Russische markten wordt ontzegd. De Chinezen en Russen trekken investeringen uit Nederland terug, waardoor onder andere de Amsterdamse vastgoedmarkt op instorten staat. En door cyberaanvallen die vooral uit China en Rusland lijken te komen, krijgt ons BNP jaarlijks een knauw van meerdere procenten.
Met een tweede termijn voor de gekozen conservatieve president, de ontvouwende *cyber arms race*, en toenemende internationale spanningen duikt de term 'Cyber Cold War' steeds vaker op in de media. Naast het Vrijheidsblok en een groep ongebonden staten in de 'Non-Aligned Movement' (het zogenaamde NAM-blok), voegen steeds meer landen zich bij Rusland en China in een coalitie van het Harmonieblok. Vooral autoritaire landen uit Azië (Noord Korea, Pakistan), het Midden Oosten (Saoedi Arabië, Turkije) en Afrika (Zimbabwe, Sudan) sluiten zich aan. Onder invloed van het zware economische weer schuren sommige westerse landen steeds dichter tegen het Harmonieblok aan. Griekenland zet als eerste de stap naar het Chinees-Russische kamp.

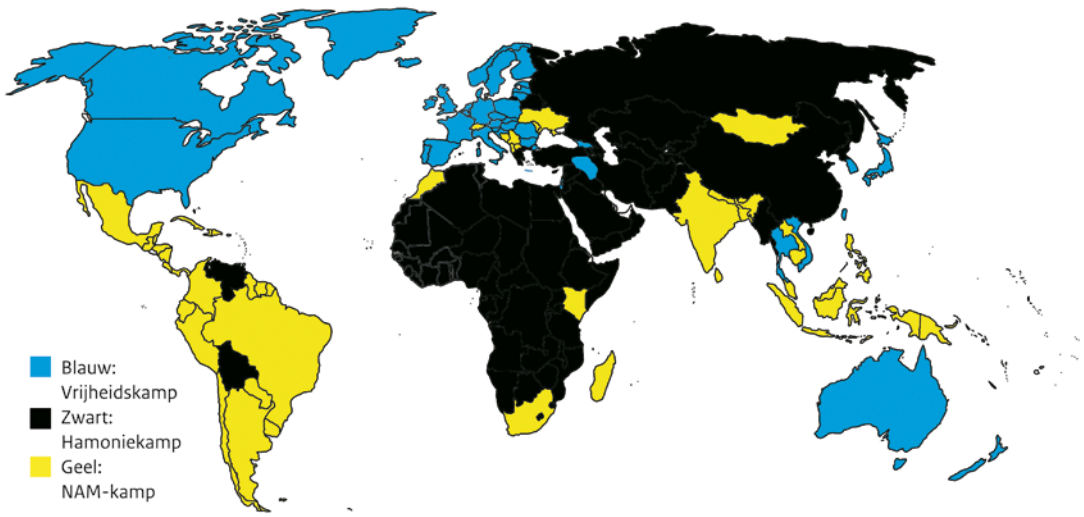
De toegezegde financiële steun en toegang tot Chinese en Russische markten bleken een *offer they couldn't refuse*. Maar de laatste jaren krabbelt de economie in het Vrijheidsblok weer langzaam op, en lijkt met name *cyberhub* Nederland te profiteren van de stijgende vraag naar cybersecurity en privacy-diensten.

Block Power

2.3 2022 - Het scenario "Block Power"

Terwijl het regeringsvliegtuig PH-KWA het Singaporese luchtruim binnenvliegt, kijkt Premier Nieuwenburg naar het doorschijnende gebogen scherm voor haar. De briefing voor de aanstaande Top tussen de drie machtsblokken – de B3 – flikkeren met berichten over het oplaaiende conflict in Taiwan. Sinds een paar jaar balanceert het land op de rand van een oorlog met China. Een Chinese hackersorganisatie kwam met bewijzen dat de aanval op de beurs van Beijing door Taiwanese hackers zou zijn uitgevoerd. En saillanter: die hackers zouden zijn getraind onder het Amerikaanse *Digital Freedom Program* (DFP). Nieuwenburg kende het geheimgehouden programma goed. Ook de Nederlandse overheid en een aantal Nederlandse

Figuur 1. Fictieve indeling van wereldkaart in kleuren geel, zwart en blauw. Geel staat voor NAM kamp, zwart voor Harmoniekamp en blauw voor Vrijheidskamp.



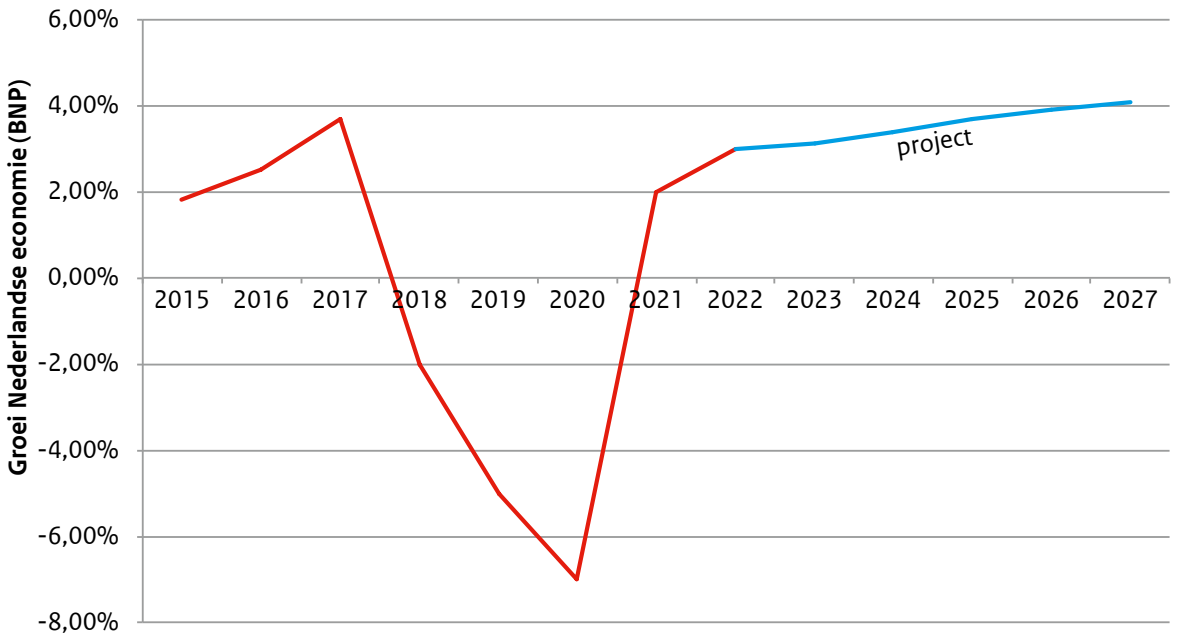
bedrijven werkten jarenlang mee aan de steun van digitale verzetsbewegingen in autoritaire regimes. Tegelijkertijd berichtten de Taiwanese kranten dat een Chinese hack een technische storing had veroorzaakt, waardoor tijdens een militaire oefening een raket op een eigen vissersboot insloeg.

Maar Nieuwenburg is vooral bezig met het bericht dat vlak voor haar vertrek op de heads-up display achter in de auto verscheen. Volgens haar collega, de Duitse Bondskanselier Kuhn, zou China met bewijzen komen dat al onze ICT *backdoors* zou Nog los van de diplomatieke schade die dat zou berokkenen, vreest Nieuwenburg voor de morele geloofwaardigheid van het Vrijheidskamp, en haar positie in het bijzonder. Twee jaar geleden werd ze als leider van de *Privacy Partij* verkozen met de belofte van Nederland een 'privacy safe haven' te maken. Na intensieve voorlichtingscampagnes, investeringsprogramma's, en stringent privacybeleid werd het vertrouwen van de Nederlandse bevolking stapvoets gewonnen.

En de florerende Nederlandse ICT-industrie, met wereldleidende multinationals zoals *IDsecure* en *Priva-See* die kapitaliseerden op de toenemende vraag naar privacy, werd Nieuwenburg de 'privacystem' van de Europese landen binnen het Vrijheidskamp. Nu dreigde datzelfde vertrouwen te paard te vertrekken en haar positie aan te tasten.

Op weg naar het vliegveld had Nieuwenburg de voorzitter van de exportbranche aan de lijn. "Van privacy kun je niet leven" had Koopman haar gezegd. En op haar scherm stond een artikel met vergelijkbare strekking en de kenmerkende kop: "Volg Gidsland Griekenland". De premier voorzag dat de lobby van de exportsector komende weken verder zou aanzwellen. Als klap op de vuurpijl had het Singaporese bedrijf *Dubidos* een overnamebod gedaan op *IDsecure*, dat alle elektronische identiteiten van Nederlandse burgers beheerde. Hoewel Singapore tot het NAM-blok behoorde, bleef het databeleid van *Dubidos* onduidelijk. Het zou niet de eerste keer zijn dat er demonstraties zouden ontstaan tegen 'vijandelijke buitenlandse overnames'. Zoals wel vaker de laatste tijd voelde Nieuwenburg zich verscheurd tussen een ogenschijnlijk economisch verstandige keuze (in dit geval: creatie van 1000 nieuwe banen) en de onzekere gevolgen daarvan (de vraag of al die persoonlijke data wel in goede handen blijft). "Focus!", dacht Nieuwenburg, sloeg haar ogen neer en zuchtte. Na een paar seconden keek ze strak naar het scherm, en terwijl ze een kringeltje in de lucht tekende, verschenen nieuwe animaties en een tekst met de kop: "*Freedom in Cyberspace: Peace and Prosperity*". In de speech die Nieuwenburg tijdens de Top namens de Europese landen gaat houden, zal ze zich fel uitlaten tegen de toenemende repressie in het Harmonieblok. Na het uitlekken van het DFP

Figuur 2. Grafiek over de groei van de Nederlandse economie (BNP) over de jaren 2015 tot 2027.



werden *special forces* en de oproerpolitie steeds vaker ingezet om protestbewegingen hardhandig de kop in te drukken. Rechts op haar scherm zag ze een filmpje waarop de Koning van Saoedi Arabië met geheven vinger de hacktivistische bewegingen toesprak als een strenge vader. Uit de ondertiteling kon ze opmaken dat het ging om de 40 opgepakte leden van de *Hackers for Freedom*-beweging. Wat met hen ging gebeuren liet zich raden. In haar speech hekelde ze verder de toenemende internetcensuur en digitale afgrenzing tussen de machtsbokken. Sommigen spraken niet langer van een *world wide web*, maar van een 'splinternet'.

Haar verhaal was echter vooral gericht aan leiders uit het NAM-kamp, zoals India, Indonesië, en Singapore. Het (weliswaar prille) economische herstel van de Nederlandse economie liet volgens haar zien dat vrijheid en groei géén *trade-off* zijn (dat argument had Nieuwenburg vaker gemaakt in debatten met de oppositiepartij *De Nieuwe Koers*, die ervoor pleitte onze 'privacy-veren' af te schudden). Het Nederlandse bedrijfsleven en onderzoeksinstellingen zouden de nieuwste ICT en encryptiemethodes ter beschikking stellen om de bevolking, bedrijven en de overheid uit deze 'scharnierstaten' te beschermen tegen toenemende cyberaanvallen. "*Flight attendants, doors to arrival and crosscheck*". Premier Nieuwenburg voelde hoe het de PH-KWA de landing inzette. Met haar vingers vormt ze een *peace*-teken. En terwijl ze daarmee naar het scherm wuifde, zag ze hoe de briefing van het scherm verdween en plaatsmaakte voor een pittoresk Hollands vergezicht.

2.4 Staatsmacht

In dit scenario vindt een verschuiving plaats in de internationale omgeving, ontstaan nieuwe machtsblokken, en zijn staten zoekende naar hun plek in een fluïde wereld. Vanwege de grote interstatelijke spanningen, de veiligheidsdreigingen en het economische zware weer, trekken westerse overheden met instemming van de bevolking meer macht naar zich toe. Nieuwe machtsconstellaties tekenen zich af, waarbij sommige landen plots een andere oriëntatie krijgen - zoals Griekenland en Saoedi Arabië, die zich meer op Rusland en China richten, terwijl landen als Koerdistan en Thailand kiezen voor het Vrijheidskamp. Binnen dat kamp verwerft de Nederlandse overheid een belangrijke positie als leider van de Europese staten die privacy hoog in het vaandel hebben staan.

Die sterke, leidende rol van de overheid is tegelijkertijd wankel. Na jarenlang slechte economische resultaten is de werkloosheid in Nederland sterk toegenomen en nemen maatschappelijke protesten tegen het pro-Amerikaanse, anti-Harmonieblok toe. Moeten we onze waarden van privacy en democratie niet inruilen voor de grote winsten die in China en Rusland zijn te behalen? Politiek tekenen zich dientengevolge ook nieuwe scheidingslijnen af. Ten tijde van de crisisjaren 2017-2020 kwam de 'Nieuwe Koers' Partij op, die pleitte voor een verminderde focus op privacybescherming, en wat in de volksmond '*het scenario Griekenland*' is gaan heten: aansluiting bij het Harmoniekamp. De partij krijgt steun vanuit de exportsector, die zware klappen krijgt te verduren door de terugvallende wereldhandel. Maar nu de Nederlandse economie weer aantrekt en Nederland ook internationaal steeds bepalender is met haar sterke privacybeleid is het vertrouwen in de overheid weer opgeklommen. In een recente peiling van een erkend onderzoeksbureau blijkt dat 67% van de Nederlandse bevolking het beleid van de minister van Cyberzaken steunt.

2.5 Cyberconflict

Cyberaanvallen nemen toe, met name spionageactiviteiten tussen de machtsblokken. De dreiging voor de Nederlandse samenleving lijkt vooral uit China en Rusland te komen. De meeste Nederlandse burgers en bedrijven hebben aan den lijve ondervonden dat cyberaanvallen reële impact kunnen hebben – van gehackte auto's tot geblokkeerde tablets die alleen door het betalen van ransomware weer vrijgegeven worden. Wie daar achter zit, en of hier sprake is van door vijandige staten georkestreerde aanvallen, blijft onduidelijk. Afgaande op de proliferatie aan criminele cyberorganisaties en samenvallende politieke en criminele doeleinden lijkt de samenwerking tussen staten en cybercriminelen steeds hechter te worden. Tegelijkertijd duiken voortdurend berichten op dat ook binnen het Vrijheidskamp grootschalige elektronische spionage plaatsvindt. De pro-privacykoers van de Nederlandse overheid betekent juist dat de mogelijkheden van de veiligheidsdiensten worden beperkt. Het publieke en politieke debat in Nederland wordt gevoed door geruchten en angst rondom spionage vanuit Amerikaanse hoek, maar ook de vraag of wij niet net als de VS meer moeten kiezen voor veiligheid.
De machtsstrijd vertaalt zich ook in een ontluikende *cyber arms race*. Nederland maakt zich hard voor een *cyber arms non proliferation treaty.* Maar voor en achter de schermen werken het ministerie van Defensie,

TNO en andere partijen uit het Cybercluster zelf ook aan de ontwikkeling van die wapens – waardoor de media de Nederlandse overheid meermaals van hypocrisie betichten. Zo'n verdrag lijkt ook weinig kans van slagen te hebben, omdat niet alleen de grootmachten, maar juist staten die slachtoffer zijn geweest van cyberaanvallen of die dergelijke aanvallen vrezen, zoals Estland, Koerdistan, Vietnam, en Taiwan, miljarden investeren in het ontwikkelen van de nieuwste cyberwapens. Zoals de spanningen in Taiwan laten zien hebben cyber-aanvallen steeds vaker materiële of grootschalige financiële gevolgen. En die spanningen tussen de blokken manifesteren zich vooral in NAM-staten als Taiwan, die zich tussen de invloedssferen van de grootmachten bevinden. Niet voor niets duikt de term *Cold Cyber War* steeds vaker op.

2.6 Internet governance

Internet governance raakt in dit scenario steeds verder versnipperd tussen de blokken. Na diplomatieke rellen rondom de vermeende partijdigheid waarmee ICANN de Internet protocollen en Domain Name Systems (DNS) toekende, richtte het Harmonieblok haar eigen DNS service op. En binnen datzelfde blok wordt al het internetverkeer sterk gecontroleerd onder het mom de staat te beschermen tegen buitenlandse invloeden. In het Vrijheidskamp blijft het internet relatief open. Staten blijven ook daar de dominante spelers, die soms in samenwerking met het bedrijfsleven, de touwtjes strak in handen houden. Wel blijven er ook binnen de blokken spanningen bestaan.

Nederland werpt zich nadrukkelijk op om privacy-wetgeving en internationale governance van een vrij en open internet te bevorderen. Het probeert zich te profileren als 'privacy safe haven': een land met de beste beschermingswaarborgen van persoonlijke gegevens. Daardoor zijn inmiddels al een aantal buitenlandse bedrijven, NGOs en zelfs 'privacy-vluchtelingen' naar Nederland gekomen. In het buitenland maakt Nederland zich hard voor een stringenter privacybeleid. En ook het streven naar een verdere verbreiding van netneutraliteitwet-geving vindt in steeds meer Europese landen opvolging.

2.7 Technologie adoptie

Door de interstatelijke spanningen en de opkomende *cyber arms race* wordt massaal geïnvesteerd in nieuwe (vooral op defensie gerichte) cybertoepassingen. Die R&D-investeringen krijgen ook hun civiele spin-off. Zo worden computers die gedachten kunnen lezen later gebruikt voor allerlei medische toepassingen – waardoor bijvoorbeeld mensen met een spraakverlamming weer kunnen communiceren.

Nederland heeft zich ondertussen ontwikkeld tot een 'ICT hub'. De *Cyber Cold War* heeft er voor gezorgd dat burgers en bedrijven zich in grote mate bewust zijn van de dreigingen in cyberspace. In het Nederlandse onderwijssysteem wordt cybereducatie een vast onderdeel. De meeste scholen bieden het vak 'Hacken voor beginners' aan. Er wordt een speciaal *cybercluster* opgezet waarbij de overheid, bedrijfsleven en kennisinstellingen samen grote maatschappelijke uitdagingen proberen aan te pakken. Mede daardoor ontwikkelde zich een levendige ICT sector die slim kon inspelen op die toenemende vraag naar cyber security en privacy. Inmiddels is onze ICT-sector goed voor meer dan tien procent van het Nederlandse BNP. Vooral de crypto-industrie is *booming*. De *cutting edge* crypto-grafie heeft een aantal multinationals voortgebracht die binnen het Vrijheidsblok hun producten en diensten aanbieden.

2.8 Indicatoren

Economie

Indicator		Assessment
Vestigingsklimaat		Gunstig (triple helix cluster, privacy-focused)
Open / gesloten		Open binnen blokken,
		gesloten tussen blokken
Duurzaamheid		Neutraal
Groei		Aantrekkend na jarenlange crisis
Arbeidsmarkt		Exportsector zware klappen
		ICT sector booming
Sociaal maatschappelijk		Nieuwe spanningen tussen pro-privacy en pro-groei bewegingen
		Ontluikend optimisme over Nederlandse positie in de wereld

Veiligheid

Indicator		Assessment
Economisch		Schade cyberaanvallen neemt toe;
		Economische spionage
Aantal / aard incidenten		Sterke stijging van cyberspionage
		Toename cybercriminaliteit (en verwevenheid staten/criminelen)
		Cyber Arms Race & Cyber Cold War
Gevoel		Stijgend vertrouwen in Nederlandse overheid
		Onveiligheidsgevoel door Cyber Cold War neemt toe
Bewustwording		Groot (mede door cybereducatie)
Mogelijkheden		Trade-off tussen privacy en veiligheidsbeleid
		Attributieproblemen
		Sterke cybersecurity regulering binnen Vrijheidskamp
		Internationale verdragen, organisaties, wereldwijde regulering onder druk

Privacy / vrijheid

Indicator		Assessment
Bewustwording		Groot (mede door cybereducatie)
Schendingen		Grootschalige incidenten
		Voortdurende speculatie nieuwe privacybreuken
		Nederland relatief goed beschermd
Technologie		Nederland koploper in encryptietechnologie en privacybedrijven
Mogelijkheden		Onduidelijk (grote vraag, veel aanbod, maar effectiviteit?)

2.9 Tot slot

Dilemma's

- Afweging economische kansen in autoritaire regimes versus waarden van vrijheid en privacy.
- Moet beleid vooral gefocust zijn op privacy of juist op veiligheid? Wat voor gevolgen heeft dat (e.g., privacy-eisen bij buitenlandse mergers & aquisitions)?
- Hoe om te gaan met grote onduidelijkheid over oorsprong aanvallen, de maatschappelijke spanningen (e.g. protesten) en speculaties in de media (e.g. complottheorieën)?
- Kun je privacy wel garanderen door supersnelle technologische innovaties en massale overheids-investeringen in cyberwapens en spionage-
- technieken?
- Hoe voorkom je dat het vertrouwen tussen bondgenoten afbrokkelt door onderlinge spionagepraktijken?
- Wat kan een klein land als Nederland betekenen in het grote machtsspel van de wereldpolitiek? Heeft het zin te streven naar het inperken van een cyber arms race?
- Hoe weerbaar/duurzaam zijn onze huidige internet governance structuren? Wat te doen als die governance implodeert?

Kansen

- Overheidsinvesteringen in cyberindustrie en -onderwijs vertalen zich in economische groei, nieuwe werkgelegenheid en innovaties.
- Nederland verkrijgt nieuw aanzien en politiek/economische/morele macht door zich op te werpen als 'hoeder van onze privacy' en zich uitbetalende investeringen in de cybersector.
- Spin-off van militaire cyberinnovaties naar civiele sector.

3 Scenario Bit Bang

3.1 Samenvatting

Door een cyberaanval op de basisregistratiesystemen[2] van de overheid raakt de samenleving als in een “slow cooker” langzaam maar zeker meer en meer ontwricht. De overheid verliest grip op de samenleving, individuen verliezen hun identiteit en daarmee kansen in de samenleving. Het is onduidelijk waar de cyberaanval vandaan is gekomen. Er zijn verschillende cyber-koninkrijkjes die elk hun eigen positieve of negatieve invloed hebben op de samenleving.

3.2 Wat ging eraan vooraf

Als gevolg van de aanhoudende stroom vluchtelingen in Europa en de toenemende terroristische dreiging van IS en vergelijkbare radicale groeperingen is Nederland in 2016 door de NAVO gevraagd om een bijdrage te leveren aan een internationale stabilisatiemacht in de regio Irak en Syrië. Anno 2022 nemen we nog steeds deel aan de NAVO missie, maar is de situatie nog steeds niet onder controle. Dit leidt tot grote onvrede van de Nederlandse bevolking, voornamelijk vanwege het ontbreken van een exit strategie. Ook de internationale moslimgemeenschap is boos vanwege de overtuiging dat wij onze Westerse normen en waarden opdringen aan de Irakese en Syrische bevolkingsgroepen. Als gevolg van aanhoudende geopolitieke, economische spanningen en een niet aflatende stroom cyberaanvallen is in 2020 een nieuwe economische crisis ontstaan. Ook proberen de BRICS-landen[3] hun invloed op de wereld te vergroten door inmenging in onze economische bedrijvigheid; BRICS bedrijven zijn actief op de Europese markt en er zijn BRICS overnames van o.a. in Nederland gevestigde ondernemingen. Binnen de politiek-economische crisis die Europa al jaren in de tang houdt, zijn bondgenoten nauwelijks geneigd elkaar een helpende hand toe te steken. De Nederlandse overheid heeft haar ICT systemen, waaronder de basisregistraties, in de afgelopen jaren beperkt doorontwikkeld en onderhouden. Nederland met zijn snelle cyberinfrastructuur en grote datahotels wordt door cybercriminelen als voornaamste aanvalsbasis gebruikt om burgers, bedrijven en financiële instellingen buiten de EU aan te vallen.

[2] http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties.

[3] BRICS-landen zijn de belangrijkste opkomende wereldeconomieën voor 2050: Brazilië, Rusland, India, China en Zuid-Afrika.

Bit Bang

3.3 2022 - Het scenario "Bit Bang"

Luitenant Steven (28) zit achter zijn bureau en is moe. Hij is net twee weken geleden teruggekomen van zijn tour in Irak. Het was zijn tweede uitzending in drie jaar tijd; als deel van de International Stabilisation Mission Middle-East (ISME) waar Nederland in NAVO-verband aan deelneemt. Nederland heeft in die periode flinke klappen te verduren gehad en er zijn sterke politieke geluiden om de Nederlandse militairen dit jaar nog uit de missie terug te trekken omdat de focus is verschoven naar de binnenlandse problematiek. Hij zucht nog eens. Het is een langslepend conflict waar Nederland in verwikkeld was geraakt, waarbij EU-lidstaten steggelen over hun bijdrage aan een uitzichtloze missie en waar China zich ook nog eens mee is gaan bemoeien. Gisteren had hij nog een hevige discussie met zijn vriendin hierover. Fijn die Chinese handreiking van bijna 10.000 IT-specialisten die ons willen helpen met het weer opbouwen van het Nederlandse stelsel aan basisregistraties na de grote hack op de overheid die in de volksmond 'Bit Bang' is gaan heten! De Tweede Kamer wil maar wat graag op het aanbod ingaan voor een gratis versnelling van het opnieuw opbouwen van alle persoonsgegevens. Want het is complex en duur en als we het zelf doen, gaat het nog jaren duren. Want zoals we al sinds het begin van deze eeuw weten: "ICT-projecten van de overheid lopen uit de hand." En omdat we niet in staat bleken de cybercriminelen tegen te houden, blokkeren vrijwel alle andere landen (BRICS uitgezonderd) de elektronische diensten die vanuit Nederland komen. Nederland is daardoor in een geïsoleerd economisch blok terecht gekomen. Maar Steven is bang dat Nederland een Trojaans Paard in huis haalt. Wat is de dubbele agenda van die Chinezen en andere BRICS-landen nu ze ook al zoveel Nederlandse bedrijven voor een prikkie hebben opgekocht?

Ja, natuurlijk is zijn vriendin vóór inmenging van de Chinezen. Zij is één van die vele slachtoffers die door de media tot 'DigiLosers' zijn gedoopt. Ze kreeg na de hack geen uitkering meer nadat ze haar baan vorig jaar was verloren in de crisis. Ze moest volledig terugvallen op Stevens inkomsten als beroepsmilitair, anders had ze niet eens eten kunnen kopen voor haar gezin met hun dochtertje Cynthia. Niemand had kunnen bedenken hoe afhankelijk burgers, bedrijven en overheden waren geworden van de Basisregistraties. En dat je bijvoorbeeld zonder een goede registratie van je identiteit en woonlocatie nergens meer aanspraak op kunt maken. Toen het uiteindelijk na vele maanden ging opvallen dat er stelselmatige fouten voorkwamen in de belangrijkste twaalf basisregistraties, was het natuurlijk te laat. Ook de back-up-bestanden van deze grote databases waren inmiddels dusdanig vervuild dat hoogstens 30% van de gegevens betrouwbaar was, maar ook dát was niet zeker. Volgens de basisregistratie bleek de premier 135 jaar oud en met twee vrouwen en drie mannen wettig getrouwd te zijn. Dat was de druppel die de Nederlandse overheid liet besluiten om de basisregistraties buiten gebruik te stellen, ondanks alle potentiële gevolgen.
Wat een chaos leverde dat op met een collectief verlies aan vertrouwen in de dingen die we tot voor kort nog voor zo vanzelfsprekend hielden. Chaos in het betalingsverkeer, winkels en op de kelderende AEX. Huizen werden onverkoopbaar, doordat de Kadastergegevens niet meer klopten. Hypotheken werden niet meer verstrekt door de banken. Uitkeringen werden niet of veel te laat uitgekeerd, met rijen noodlijdende gezinnen en AOWers bij de voedselbanken tot gevolg. Ziekenhuizen namen nog wel patiënten aan, maar de afrekening bij de verzekeraars liep hopeloos in soep, waardoor deze op hun beurt weer claims bij de Staat legden. Gisteren kreeg Stevens vriendin bijvoorbeeld pas na vele weken te horen dat Cynthia via een handmatige administratie eindelijk aangemeld was voor de basisschool! Alleen maar doordat het Basisregistratie Personen (BRP) systeem onbruikbaar was geworden en de school zo slim was om snel over te stappen op dat nieuwe gecrowdsourcede initiatief van Social Media IDentity (SMID) waarbij bekenden elkaars identiteit authentiseren!

De nationale politie en de AIVD zitten met de handen in het haar nu het criminele circuit vol is gedoken op uitbuiting van deze chaotische situatie. Fraude met elektronische identiteiten maakt de chaos nog groter. Banken geven geen leningen meer uit omdat mensen niet meer kunnen bewijzen wie ze zijn. Er is een levendige (illegale) online ruilhandel ontstaan en er wordt tegenwoordig online meer betaald in BRICScoins dan in euro's.

De overheid onderzoekt nog steeds met man en macht naar de daders die achter de Bit Bang hack zaten. Was het omdat we bijdroegen aan de

NAVO-missie? De eerste aanwijzingen duidden erop dat er een staatsmacht achter zat, maar nieuwe inzichten geven een sterk vermoeden dat het een groep scriptkiddies of hacktivisten is geweest, die zich heeft uitgeleefd op de sterk verouderde en matig onderhouden ICT-infrastructuur van de overheid. Steven is bang dat we er nooit helemaal achter zullen komen. Wel is zeker dat veel migranten en vluchtelingen die naar Nederland komen, een gewild afnemer zijn van de valse identiteiten die door criminele bendes (in de volksmond Bit-Bang-Gangsters geheten) worden verstrekt. We weten straks niet eens meer wie een echte Nederlander is en wie niet!

Steven staat op en loopt naar de machine om nog maar een kop koffie te halen. Koffie die zijn vriendin met veel korting kon kopen in de supermarkt als ze maar akkoord ging dat het enorme buitenlandse concern haar koop- en eetgedrag en dat van hun dochtertje kon monitoren. Wat ze met al die data gaan doen straks, laat zich natuurlijk raden. Steven neemt nog maar een flinke warme slok en schud meewarig zijn hoofd. Zijn wereld en dat van zijn gezin is flink door elkaar geschud.

3.4 Staatsmacht

De overheid hapert na de hack op de basisregistratiesystemen. Het onderuitgaan van het stelsel van deze basisregistraties veroorzaakte een kettingreactie binnen de overheid en initieerde een maalstroom aan problemen. De overheid weet niet waar te beginnen met puinruimen. Door onderlinge verdeeldheid in de politiek blijven heldere beleidslijnen en leiderschap achterwege; het vertrouwen van de burger in de staat brokkelt verder af. Het is duidelijk dat Nederland in tijden van economische crisis hulp kan gebruiken, maar wat te doen met de handreiking van China? Andere Europese landen lijken het te druk te hebben met hun eigen problemen in het economische zware weer. Daarnaast hebben zich een aantal nieuwe grote multinationals zoals het Zuid-Afrikaanse Wipmat[4] en het Portugese VdC[5] gevormd (en zijn bestaande overgenomen) waar we ook economisch sterk van afhankelijk zijn (want het levert veel banen op). Deze multinationals hebben zich gestort op het verzamelen en analyseren van data over onze levenspatronen als burger en werknemer. Ons koopgedrag, onze voorkeuren en dagelijkse bezigheden worden als big data geanalyseerd om vervolgens hierop in te spelen met speciale aanbiedingen aan producten en diensten van deze grote conglomeraten. De overheid heeft moeite hiertegen een vuist te maken, wat het vertrouwen van de burger in de overheid nog meer laat inboeten. En in tijden van schaarste lijken de meeste burgers hun privacy snel in te ruilen voor een schijnbaar voordeeltje.

3.5 Cybercomflict

Attributie van de grote Bit Bang hack is zeer lastig gebleken. Het lijkt erop te duiden dat een groep hacktivisten of scriptkiddies met vergelijkbare ‘cyber-capabilities’ onze samenleving heeft willen verstoren, maar het is zeer moeilijk te achterhalen. Onder de grote druk van politici ruziën de kopstukken van Defensie, het OM en de politie met elkaar omdat er niet met zekerheid kan worden gezegd wie er precies achter de hack zit. Er wordt modder gegooid naar Defensie, omdat zij, naar eigen zeggen volgens hun mandaat, niet terug mogen slaan. Het OM en de politie kunnen geen mensen of groepen vervolgen wegens gebrek aan sluitend bewijs. En er wordt druk op BuZa uitgeoefend om maar sancties in te stellen tegen verdachte groepen en staten, hetgeen weer diplomatieke verontwaardiging oplevert.

In de binnenlandse politiek wordt de schuldvraag door en in het parlement gezocht; wie is verantwoordelijk voor het achterblijven van de cybersecurity maatregelen in de Basisregistratiesystemen? Waarom moet de heropbouw van de basisregistratie databases zeven jaar duren? Het opstappen van de minister van BZK was niet genoeg; uiteindelijk is de regering ook door het Bit Bang incident gevallen. Met de aanstaande verkiezingen voor de deur en de grote groep ontevreden burgers kan de samenstelling van een nieuwe regering er wel heel anders gaan uitzien.

Door de databases van de basisregistratiesystemen te corrumperen, is de identiteit van burgers en hun bezittingen niet of moeilijk te bewijzen. Veel processen en procedures die op deze basisregistratie leunen, werken niet meer, of niet goed. Een situatieversterkende factor is de toenemende rol van de georganiseerde misdaad die welig tiert bij de ontstane chaos en de ontstane vraag naar nep-identiteiten.

[4] Wipmat (Trampoline in het Nederlands) is een Zuid-Afrikaanse multinational voor online loopbaan- en levensbegeleiding.

[5] Vazamentos do Cérebro is een Portugese big data multinational die in het Engels ook wel Brain Leaks wordt genoemd.

3.6 Internet governance

Sinds 2015 is er veel veranderd op het vlak van internet governance. Landen kunnen (mede veroorzaakt door de sterke lobby van grote bedrijven) het niet eens worden over nieuwe regels zoals privacyrichtlijnen, diverse nieuwe EU standaarden en nieuwe mogelijkheden voor het internationaal vervolgen van cyber-criminele activiteiten. Daarom heeft Nederland, na langdurige internationale beschuldigingen als cybercrime-faciliterend land nr. één en om uit ons economisch isolement te komen, recentelijk gekozen voor een harde aanpak met een beleid waarin security centraal staat. Zo heeft Nederland zich gecommitteerd aan de onlangs gepubliceerde stringente EU-cybersecurityrichtlijnen en weinig aandacht meer geschonken aan privacy versterkende beleidsmaatregelen. Nederland heeft zich daarmee sterk geïsoleerd van de opkomende nieuwe economieën die gebaseerd zijn op het nieuwe cyberdenken waar privacy een veel sterker belang toegedicht wordt. Waar de overheid niet heeft doorgepakt op privacy, schieten daarentegen nieuwe pro-privacy burgerinitiatieven als paddenstoelen uit de grond. Enerzijds Anonymous-achtige groeperingen; zij zijn tegen de verkregen vergrote macht van de grote bedrijven met hun sympatiek lijkende Big-Brother en Big Data oplossingen nu de Staat hapert in het uitoefenen van haar governance. Anderzijds worden creatieve nieuwe oplossingen voor hedendaagse problemen door betrokken burgers gecrowdsourced.

3.7 Technologie adoptie

Door een verlies aan vertrouwen in bestaande technologie-oplossingen zoals e-ID en Internetbankieren, hebben veel Nederlanders snel andere vormen van identificeren en betalen geadopteerd. Nieuwe vormen van online ruilhandel en de omarming van crypto-currencies zoals de BRICScoin waarmee ze minder afhankelijk zijn van traditionele banken, worden snel omarmd. Dit fenomeen heeft ons geïsoleerd van de wat meer conservatieve landen die nog met standaard valuta handelen. Tegelijkertijd lijkt hiermee ook de rol van de Nederlandse financiële sector op het wereldtoneel af te gaan nemen.
Wel heeft de ontstane crisis een zoektocht naar nieuwe en innovatieve oplossingen gestimuleerd onder burgers en het MKB. Er gaan al wel geluiden op onder experts of deze nieuwe oplossingen op den duur zelf wel veilig en te vertrouwen zijn.

3.8 Indicatoren

Economie

Indicator		Assessment
Vestigingsklimaat		Laagdrempelig
Open / gesloten		Open economie
		In economisch isolement geraakt
Duurzaamheid		Geen bewuste focus
Groei		Crisis beperkt economische groei
Arbeidsmarkt		Groei door buitenlandse bedrijven
		Krimp door crisis
Sociaal maatschappelijk		Onrust onder burgers en bedrijven

Veiligheid

Indicator		Assessment
Economisch		Krimp door Bit Bang hack
		Verslechterd internationaal imago
Aantal / aard incidenten		Toegenomen
Gevoel		Bevolking heeft vertrouwen in overheid verloren
		Internationale gemeenschap ziet Nederland als faciliterend platform voor cybercrime
Bewustwording		(Tijdelijk) hoog door cyberincidenten
Mogelijkheden		Burgerinitiatieven
		Implementeren EU cybersecurityrichtlijnen om cybercrime activiteiten te verminderen
		Interne strijd overheid

Privacy / vrijheid

Indicator		Assessment
Bewustwording		(tijdelijk) Hoog door cyberincidenten
Schendingen		Grootschalige ID fraude
Technologie		Te weinig onderhoud en innovatie door overheid in digitale systemen
Mogelijkheden		Burgerinitiatieven
		Bewust afgeweken van privacy in het nieuwe cyberdenken

3.9 Tot slot

Dilemma's

- Een open economie en een lokaal ingericht vestigingsklimaat voor ICT bedrijven versus het uitblijven van de aanpak van de Nederlandse ICT infrastructuur dat facilitair gebruikt wordt voor cybercrime activiteiten in de rest van de wereld.
- Keuze voor vergroot (cyber)veiligheidsbeleid en open economie versus de negatieve impact daarvan op de privacy van burgers.
- Open economie waar bedrijven hun verdienmodel focusseren op big data analytics schaadt de privacy van burgers waardoor vertrouwen in overheid vermindert.
- Digitalisering van overheidsdiensten (bijv. Basisregistratiesystemen) levert efficiencyvoordelen op, maar creëert ook nieuwe (cyber)risico's.
- Wat is de juiste vervangingsstrategie van ICT? Kiezen we voor incrementele vervanging van oude ICT of wordt het in één keer vervangen?
- Een handreiking van een BRICSland in tijden van crisis versus dubbele agenda's (korte versus lange termijn).

Stakeholders

- BRICS-landen.
- Multinationals, grote conglomeraten.
- Burgers.
- Activistische groeperingen.
- Overheidspartijen.
- Veiligheidsdiensten overheid.

Kansen

- Burgerinitiatieven en crowdsourcing.
- Creativiteit wordt gestimuleerd door een crisis in een open economie.
- Alternatieve valuta voor continuering betalingsverkeer.

4 Scenario Splitting society

4.1 Samenvatting

De Nederlandse samenleving is hyperconnected. Alles en iedereen is wereldwijd met elkaar verbonden. Er is een grote groei in een nieuwe hightech industrie, maar niet iedereen heeft daar baat bij. 'Digibeten' kunnen de verregaande digitalisering niet meer aan. Educatie heeft niet genoeg aandacht gekregen. Er ontstaat maatschappelijke onrust en er is een wankel evenwicht tussen veiligheid en onveiligheid.

4.2 Wat ging eraan vooraf

De Nederlandse regering heeft jarenlang ingezet op het stimuleren van een hightech kenniseconomie. Vooral cyberbedrijven hebben geprofiteerd van het Topsectorenbeleid. Hieraan heeft ook de duurzaamheidsstimulans bijgedragen; het Nederlandse concept van energie-neutrale cyberdiensten heeft wereldwijd klanten opgeleverd. Enkele Nederlandse cyberbedrijven zijn uitgegroeid tot grote, internationaal zeer succesvolle spelers en de Nederlandse economie is sterk van hen afhankelijk geworden. Het MKB drijft ook deels op deze bedrijven, als toeleverancier dan wel via doorontwikkeling van basistoepassingen van de grote bedrijven.

Daarnaast heeft de overheid verregaande digitalisering gestimuleerd. Het 'Internet-of-Things' heeft Nederland in razend tempo veroverd; alle denkbare apparatuur is digitaal verbonden. Fysiek winkelbezoek is vrijwel verleden tijd geworden, bestellingen worden vrijwel altijd online gedaan – in sommige gevallen zelfs automatisch door zelfdenkende apparatuur. Dienstverlening is in grote mate verschoven van mensenwerk naar digitale processen. Vrijwel alle overheidsdiensten waarvoor burgers vroeger naar een fysiek loket moesten, zijn nu digitaal belegd: van begeleiding bij een werkloosheidsuitkering tot het aanvragen van vergunningen, alles verloopt via Internet. Onderwijs en medische indicatiestelling gebeuren eveneens grotendeels op afstand. Dit heeft de efficiëntie van de overheid flink vergroot en de belastingdruk sterk verlaagd – hetgeen het economische vestigingsklimaat extra stimuleert. Er blijken echter ook nadelen aan deze verregaande cyberficatie te kleven.

4.3 2022 - Het scenario "Splitting society"

"Dit is het NPO diginieuws van 6 november 2022. In de exit-polls van de Enige Kamerverkiezingen lijkt de Menselijke Maat Partij (MMP) de grote winnaar met 42 procent van de stemmen. De recente affaire met de gehackte verzorgingsrobots die tot tientallen te heet gedouchte slachtoffers leidde, heeft de partij geen windeieren gelegd.

Lijsttrekker Mirjam Geluk: 'Het volk heeft gesproken. De ontdigitalisering gaat van start. Met hogere belasting op de winst van de grote cyberbedrijven en de buitensporige salarissen van hun werknemers gaan we de mens terugbrengen in zorg, onderwijs en overheid. We kunnen niet langer toestaan dat een derde van de bevolking buitenspel staat en in grote problemen komt omdat met algoritmes niet valt te discussiëren. De cybercriminelen, privacyschendingen en op hol geslagen complexiteit moeten tot stoppen worden gebracht.'

Onze premier erkende zijn electorale verlies, maar waarschuwde meteen voor het vertrek van alle grote cyberbedrijven uit Nederland naar cyberwalhalla Kenia, waar cyberbedrijven aan geen enkele regelgeving hoeven te voldoen. De premier: 'Onze inzet op het versterken van cybereducatie begint net aan te slaan, helaas heeft de kiezer dat niet op waarde kunnen schatten. De MMP begrijpt niet dat Nederland zal terugvallen naar een Derde Wereldland als ze de cyberbedrijven waarop onze economie drijft, de grens over jaagt.'

In de vele achterstandswijken en op het platteland is de overwinning van de MMP luidruchtig gevierd. Werklozenfederatie Ontslagen (Semi-)Ambtenaren Belangen (OSAB) riep op tot kalmte om de gebruikelijke rellen en plunderingen te voorkomen. Niettemin heeft de politie extra drones met automatische gezichtsherkenning ingezet."

4.4 Staatsmacht

In dit scenario is de Nederlandse overheid enorm gekrompen. Vergaande automatisering heeft tot grootschalige reductie van het aantal ambtenaren en semiambtenaren geleid. De efficiëntieslag (en bijbehorende belastingverlaging) heeft de overheid echter ook vervreemd van een groeiend deel van de samenleving. Lager opgeleiden, ouderen en sociaal zwakkeren hebben de cyberficatie niet kunnen bijbenen en staan min of meer buiten de samenleving. Doordat zij hun gegevens niet (kunnen) invoeren in de overheidssystemen vallen zij deels buiten het zicht (en wellicht macht) van de overheid. Dit effect wordt nog vergroot door de toenemende burgerlijke ongehoorzaamheid, gepropageerd door een groeiende protestbeweging tegen wat men noemt 'doorgeschoten digitalisering'.

De groep 'digibeten' overlapt deels met de grote groep werklozen wiens werk door digitalisering is vervallen. Jongeren blijken via onderwijs op afstand te weinig sociale vaardigheden mee te krijgen, hetgeen tot groeiende maatschappelijke problemen leidt. In achterstandswijken en op het platteland is in toenemende mate sprake van verzet tegen de overheid, evenals wetteloosheid en anarchistische taferelen. Op deze afnemende fysieke veiligheid heeft de sterk gedigitaliseerde overheid geen duidelijk antwoord, zeker niet als het personen betreft die in de digitale bestanden van de overheid (vrijwel) afwezig zijn.

Bovendien is de economische afhankelijkheid van enkele zeer grote (deels in Nederland gevestigde) cyberbedrijven zo gegroeid, dat zij grote invloed op het landsbestuur hebben. Deze bedrijven, samen het van hen afhankelijke deel van het MKB, zijn inmiddels goed voor een aanzienlijk deel van het Bruto Nationaal Product. De werknemers van deze bedrijven (vooral aan de top) verdienen buitensporig hoge salarissen. Zodra voor de grote cyberbedrijven minder profijtelijk beleid wordt geopperd, dreigen zij met vertrek naar andere landen waardoor de Nederlandse economie zou instorten. Hierbij wordt vaak het voorbeeld van Luxemburg aangehaald, waar de economie in 2017 dramatisch instortte na strengere regelgeving voor financiële instellingen en prompt alle bedrijven vertrokken.

Overigens doen de ontwikkelingen in Nederland zich eveneens voor in diverse andere sterk gedigitaliseerde landen. Een internationale anti-digitaliseringsbeweging, NewOccupy, probeert de protesten in de verschillende landen te coördineren. De

doelstellingen van NewOccupy worden in Nederland nog veelal als te radicaal bestempeld, maar vooral onder jongeren blijkt er toch groeiende steun voor te zijn.

4.5 Cyberconflict

Nederland heeft in dit scenario vooral te maken met economisch cyberconflict. Er is een cyberspionage-wedloop gaande tussen de grote cyberbedrijven in de wereld, en ook de in Nederland gevestigde bedrijven ervaren regelmatig dat hun kostbare innovaties op het terrein van quantumcomputer-ontwikkeling en big data mining & analytics systemen net iets eerder op de markt worden gebracht door buitenlandse concurrenten. Andere landen beschuldigen nadrukkelijk ook de Nederlandse bedrijven van cyberspionage en -sabotage, maar de Nederlandse overheid weigert tegen de bedrijven op te treden onder het mom van gebrek aan bewijs. Dit leidt tot de nodige diplomatieke spanningen met andere landen.

Nederland is bovendien een belangrijk doelwit van cybercriminelen. Niet alleen vanwege de hoge digitalisering van de samenleving, maar ook omdat een deel van de bevolking een makkelijke prooi is. De mensen die het digitaliseringsproces niet hebben kunnen bijbenen trappen eenvoudig in cyber-criminele tactieken of vertonen door gebrekkig begrip zelf onveilig cybergedrag. Zij zijn niet alleen het slachtoffer van financiële en identiteitsfraude, maar ook kan regelmatig via hen toegang worden verkregen tot netwerken van bedrijven en organisaties. Onderzoekers van de Algemene Rekenkamer constateerden dat door de overheid betaalde uitkeringen in toenemende mate niet geheel bij de juiste persoon terecht komen, maar door cybercriminelen deels wordt doorgesluisd naar het buitenland.

De Nederlandse regering heeft ook flink geïnvesteerd in cyberficatie van de krijgsmacht, ten koste van klassiekere krijgsmachtonderdelen (de onderzeeboten zijn bijvoorbeeld definitief wegbezuinigd). Er woedt een politieke discussie over het regeringsvoornemen om ook de kosten van het sterk gegroeide Defensie Cyber Commando te verminderen door meer op 'pooling & sharing' met bondgenoten in te zetten – tegenstanders vinden dat teveel veiligheidsrisico omdat ook bondgenoten spioneren. Nederland is in 2022 nog niet betrokken geraakt bij werkelijke cyberconflicten.

4.6 Internet governance

Wereldwijd bestaat een grote diversiteit aan regelgeving op het terrein van cyberactiviteiten. In sommige landen is alles mogelijk, zoals Kenia dat dankzij de zeer liberale internetwetgeving is opgeklommen tot één van de leidende economieën wat betreft cyberinnovatie. Andere landen hanteren echter weer zeer strenge regels, maar in verschillende opzichten: sommige landen strijden actief tegen inbreuken op privacy en veiligheid, terwijl andere landen juist strenge regels hebben die staatsinmenging mogelijk maken, officieel om staatgevaarlijke activiteiten te voorkomen maar economisch gewin speelt regelmatig ook een rol.

Nederland zit een beetje in het midden, er zijn weliswaar wetten en regels die de internetvrijheid en privacy moeten veilig stellen, maar in de praktijk blijkt dat Nederlandse cyberbedrijven veel ruimte krijgen om die regels in hun voordeel te interpreteren. De ambivalentie van de overheid ten aanzien van de frictie tussen economische belangen en veiligheid op cybervlak blijkt onder meer uit de kritiek die de recent opgerichte Inspectie Cyber Veiligheid oogst. Deze nationale toezichthouder heeft volgens velen te weinig krachtige middelen tot haar beschikking om een vuist te kunnen maken tegen bedrijven die het minder nauw nemen met cyberveiligheid. Ook internationaal dragen Nederlandse diplomaten de officiële Nederlandse cybernormen weinig krachtig uit omdat dit economische belangen kan schaden. De ambivalente houding van de overheid wakkert de antidigitaliseringsprotesten in de Nederlandse samenleving alleen maar verder aan.

4.7 Technologie adoptie

Cyberficatie heeft in Nederland een hoge vlucht genomen, op dit vlak hoort het land tot de voorlopers in de wereld. De beleidsinzet op een hightech economie is effectief geweest, het land is zelfs grotendeels afhankelijk geworden van enkele grote hightech bedrijven die internationaal zeer succesvol zijn (deze bedrijven zijn echter niet locatie-gebonden en dus eenvoudig te verplaatsen naar het buitenland). Een opkomende markt lijkt het leveren van beter beveiligde cyberproducten en -diensten, maar de start-up bedrijfjes die zich hiermee bezig houden, lijken voortdurend te worden tegengewerkt of overgenomen door de grote cyberbedrijven. De groei van de cyberbedrijfstak en de verregaande digitalisering van de overheid

hebben wel tot een scheefgroei in de economie gezorgd; relatief veel non-cyberarbeid in de dienstensector is overbodig geworden of geoutsourcet naar het buitenland. Ondanks het positieve economische vestigingsbeleid (stimulatie-maatregelen voor hightech bedrijven en duurzaam-heidsinitiatieven, lage belastingdruk, flexibele opstelling jegens regelgeving voor cyberbedrijven) kampt Nederland met een hoge werkloosheid en een groeiende inkomensongelijkheid. De grote leegstand van kantoren en winkelruimtes vormt een apart probleem.

De technologische adaptie is bovendien niet overal in de samenleving even hoog. Een niet onaanzienlijk deel van de bevolking is gedurende het snelle proces van cyberficatie afgehaakt. Redenen hiervoor zijn gebrek aan kennis (er is veel kritiek op het Nederlandse onderwijssysteem), gebrek aan vertrouwen (versterkt door cyberincidenten zoals schadelijke hacks, spionage, invloed van bedrijven en privacyschendingen door de overheid zelf), en economische malaise (de werkloosheid is flink gestegen doordat er veel minder vraag naar arbeid is). Deze tweedeling in technologische adoptie veroorzaakt groeiende maatschappelijke spanningen. Naast de roep om het deels terug-draaien van digitaliseringsprocessen en het sterk verbeteren van cyberveiligheid, is er ook steeds meer steun voor protectionistische maatregelen om het wegvloeien van arbeidsplaatsen naar het buitenland te stoppen.

4.8 Indicatoren

Economie

Indicator		Assessment
Vestigingsklimaat		Aantrekkelijk vestigingsklimaat
Open / gesloten		Open economie
Duurzaamheid		Duurzaamheid is prioriteit
Groei		Trend naar eenzijdige cybereconomie
Arbeidsmarkt		Vraag naar arbeid daalt
Sociaal maatschappelijk		Sociaal-maatschappelijke onrust

Veiligheid

Indicator		Assessment
Economisch		Bedrijfsspionage flinke schadepost
		maar spioneren zelf ook
Aantal / aard incidenten		Veel cybercrime
		Maar geen cyberoorlog
Gevoel		Sterk stijgend onveiligheidsgevoel
Bewustwording		Lage bewustwording bij ‘digibeten’
Mogelijkheden		Sterke cyberdefensie
		maar bedrijven & criminelen vrij spel

Privacy / vrijheid

Indicator		Assessment
Bewustwording		Bewustwording stijgt,
		maar veel afhakers
Schendingen		Toename ernstige privacy schendingen
Technologie		Weinig investeringen in veiligheidstechnologie
Mogelijkheden		Toezicht overheid faalt

4.9 Tot slot

Dilemma's

- Cyberficatie van de samenleving lijkt onontkoombaar, maar hoe kunnen alle bevolkingsgroepen aangesloten worden houden?
- Digitalisering van overheidsdiensten levert een enorme efficiëntieslag op, maar hoe kan vervreemding tussen overheid en (minder digitaal bedreven) burgers voorkomen worden?
- Hoe verhoudt een aantrekkelijk economisch vestigingsklimaat zich tot een krachtig staatstoezicht op omgang van bedrijven met cyberveiligheid en privacy?
- Moet en kan de overheid optreden tegen commerciële cyberspionage jegens èn door Nederlandse bedrijven?
- Hoe te voorkomen dat enkele grote cyberbedrijven zoveel macht naar zich toe trekken dat ze kleinere spelers uit de markt kunnen drukken?
- Hoe te voorkomen dat digitalisering leidt tot zoveel onnodig gemaakte beroepen dat de structurele werkloosheid fors stijgt?
- Hoe te voorkomen dat cyberbedrijven bij enige tegenwind vanuit de overheid meteen vertrekken naar andere landen?

Kansen

- Digitalisering verhoogt efficiëntie overheid, verlaagt belastingdruk en verbetert vestigingsklimaat.
- Cyberbedrijven zijn niet locatiegebonden, dus zijn vatbaar voor vestigingsstimulansen.
- Goede cybereducatie helpt maatschappelijke problemen voorkomen.
- Cyberficatie kan duurzaamheid ten goede komen.

5 Scenario Safe Haven

5.1 Samenvatting

De Een aantal samenlevingen, waaronder de Nederlandse, liepen voorop in de wereld in de adaptatie van ICT en door ICT mogelijk gemaakte technologische ontwikkelingen. In 2017 vond een cyberconflict plaats en werd duidelijk dat de Afrikaanse cybermaffia een zware greep heeft op de sterk genetwerkte samenlevingen. Dit heeft geleid tot nieuwe publieke en private samenwerkingsverbanden, zowel op lokaal als internationaal niveau om aan de cyberkwetsbaarheid tegenwicht te bieden. Nederland behoort tot dat deel van de wereld waar nieuwe standaarden voor cyberveiligheid en privacybescherming en wet- en regelgeving leiden tot een veiliger (deel van) cyberspace. Dit heeft geleid tot een vorm van kristallisatie van nieuwe governance-structuren en machtsverhoudingen. Enerzijds geeft dit meer vertrouwen in producten, diensten en overheid, anderzijds belemmert dit de technologische innovatie- en economische groeisnelheid, zoals die in andere landen plaatsvindt waar politiek en overheid veel liberaler met ICT-innovatie omgaan.

Safe Haven

5.2 2022 - Het scenario “Safe Haven”

VIJF JAAR LATER:
KOMEN WE NOG UIT DE CYBERSTROOP?
Joost Hamel, de elektronische zaterdagbijlage van de NRC, 17 september 2022

Verbaast u zich ook over de nieuwsberichten over de volledig geïntegreerde ICT-samenlevingen van Singapore, Taiwan en Sri Lanka? Waarom mag men daar wel een geur- en smaakdispenser aan het internet koppelen zodat je thuis de digitaal te bestellen maaltijd kunt ruiken en proeven? Waarom heeft u nog vijftien pasjes nodig, terwijl in Singapore een onderhuids geïnjecteerde chip voldoende is voor alle authenticatie- en betaalfuncties? Waarom kunnen alcoholisten hier nog steeds slachtoffers op de weg maken, daar waar in Taiwan de slimme auto niet start als de bestuurder een alcoholische versnapering heeft genuttigd? Uw verslaggever ging op onderzoek uit.

In 2014 had 98 procent van de Nederlandse huishoudens een breedbandinternetaansluiting. Ook op mobiel internetten via 4G liep Nederland wereldwijd aan kop. Wereldwijd gezien hadden we de meeste sociale-mediacontacten. We lieten alleen Estland en Finland aan ons voorgaan qua elektronische dienstverlening door de publieke sectoren. Ook de private sector speelde in op de snelle technologische ontwikkelingen door hun digitale diensten tot bijna niet meer inzichtelijke ketens te koppelen.
Met onze Nationale Cyber Security Strategie probeerden we publiek en privaat de negatieve aspecten in de greep te houden. De waarschuwingen van vele privacy- en cyberveiligheidsdeskundigen ten spijt, was er - achteraf gezien - te weinig aandacht voor de cyberkwetsbaarheden van onze digitaliserende samenleving. De snelle adaptatie van *Internet-of-All-Things*, zoals het nu heet, maakte onze samenleving, net als die van andere landen, alleen maar meer kwetsbaar. Organisaties, politiek, 'de overheid', u en ik lagen daar niet echt wakker van, een enkeling uitgezonderd. Organisaties polderden veel liever dan dat we samen eens echt doorpakten om de privacy- en veiligheidsproblematiek volledig onder controle te brengen. Feitelijk dachten we allemaal dat een andere partij wel voldoende greep en toezicht zou organiseren om het niet uit de hand te laten lopen. De economische voordelen waren daarbij groot: wij kwamen innovatief met zijn allen veel sneller uit de bankencrisis dan gedacht.

Onuitwisbaar herinnert u zich 17-11-17, het uitbreken van het eerste echte cyberconflict *"Militaires multinationaux sous la conduite des têtes de fromage, rentrez dans votre pays!"* De Franse samenleving werd tot diep in de kern geraakt door de irreguliere cybertroepen van AQIM (Al Qa'ida in the Islamic Maghreb). De schokkende beelden van de gevolgen van stroomuitval, verstoring van logistieke stromen (waardoor supermarkten wel wc papier maar geen voedsel afgeleverd kregen), falende rioleringssystemen, uitval van treinen en metro's en onbetrouwbaar drinkwater staan gegrift op ons aller netvlies. De gevolgen zijn bekend. De door Frankrijk geleide stabilisatiemacht in Mali werd teruggetrokken.
Dat onze Nederlandse overheid besloot om onze troepen ook uit Mali terug te trekken heeft ons land groot gezichtsverlies opgeleverd bij veel Afrikaanse en Aziatische landen. De cyberaanval op de chemische fabriek in Kaatsheuvel met een veertigtal slachtoffers tot gevolg en een paar DDoS-aanvallen kon volgens hen toch geen reden zijn voor het in de steek laten van Afrika?

Eind 2017 werd duidelijk dat de breed in cyberspace opererende Afrikaanse cybermaffia achter de sterk toenemende identiteitsfraude en cyberoplichting in Westerse landen zit. In Nederland liepen de cybercrime en –spionagekosten snel op van bijna 1,5% BBP in 2014 naar 3,4% in 2017. De verwevenheid van deze onderwereld met onze bovenwereld bleek groter dan gedacht. Uit kringen rondom onze inlichtingendiensten bleek dat er sterke aanwijzingen waren dat AQIM gebruik maakte van de Cyber-Attack-as-a-Service diensten van de cybermaffia.
De roep vanuit het MKB, vitale infrastructuurbedrijven en burgers voor meer cyberveiligheid en privacy groeide en uitte zich in *unplugged*-acties waarbij bedrijven en burgers weigeren nog langer informatie elektronisch aan te leveren. Overheid en parlement reageerden hier in eerste instantie afwachtend op.
Het uitlekken van een drietal voor de overheid ontwikkelde scenario's uit 2015 die het mogelijke cyberrisico voor de Nederlandse samenleving goed samenvatten versterkte de politieke druk en de druk van het bedrijfsleven om de cyberonveiligheid eens en voor altijd een halt toe te roepen. Tijdens de in allerijl in het World Forum in Den Haag bijeengeroepen "World Summit on Cyberspace 2018" werd door een kopgroep van veertien Europese landen, de C14, en een aantal grote spelers uit de ICT-industrie, besloten tot de "War on Cyberspace Insecurity". Landen zoals België, Duitsland, de VS, Rusland, Taiwan en India en aantal private partijen zien niets in die aanpak. Zij blijven ondanks het Wild West risico een open cyberspace nastreven.

Nu, vijf jaar na de start van onze War on Cyberspace Insecurity zouden we ons eens kritisch moeten afvragen wat dit voor ons betekent, waarom onze ICT-innovatie veel trager loopt dan elders. Wat staat daar eigenlijk tegenover? Waarom zouden we de cyberstroperigheid moeten accepteren? Is het wel zoveel veiliger geworden in cyberspace? Zijn we niet doorgeslagen in de War on Cyber Insecurity?

5.3 Staatsmacht

In de aanpak van de War on Cyberspace Insecurity heeft Nederland de Raad van Europa een nieuwe versie van de Convention on Cybercrime (ook wel Boedapest Convention) voorgelegd. Met een Europese kopgroep aan landen waaronder Frankrijk is een snelle besluitvorming in de Raad doorgedrukt. Daarbij werden de landen ondersteund door de SEGRIT pressiegroep van ICT-producten en

-dienstenleveranciers. In de strijd tegen cybercriminaliteit worden naast versterking van de bestaande afspraken nieuwe maatregelen geïntroduceerd. Deze moeten binnen drie jaar na ratificatie worden doorgevoerd. Ten eerste dient alle software aan onafhankelijke testen te worden onderworpen. Pas na het verkrijgen van een cyber- en privacy-veilig certificaat mag deze op de markt worden gebracht. Dit geldt ook voor alle in ICT-functies verstopt in de *Internet-of-All-Things*. Denk aan de software in uw thermostaat, een deurbel en uw nieuwe ledlampen. Ten tweede dienen alle sectortoezichthouders scherp toezicht te houden op de cyber- en privacy-veiligheid van organisaties en de cyberveiligheid van *industrial control systems* (denk bijvoorbeeld aan raffinaderijen, robots en voertuigen) zodat ook veiligheid van personen, dieren en milieu gewaarborgd zijn. Ten derde het invoeren van een e-rijbewijs voor alle burgers. Ten vierde de verplichting voor bedrijven en overheid tot het afschermen en veilig houden van de nationale cyberspace door het verplicht gebruik van cyber security standaarden. Ten vijfde wordt een Europese CyberAutoriteit (ECA) opgericht die onderzoeksplicht heeft naar ernstige cyberincidenten à la de FAA in de luchtvaartindustrie. ECA aanbevelingen zullen verplicht moeten worden doorgevoerd in nationale regelgeving.

Daarnaast bevat de Convention on Cybercrime van Den Haag een aantal regels waaraan wereldwijd opererende ICT-bedrijven zich kunnen verbinden in de aanpak van de War on Cyberspace Insecurity. De kern is commitment om producten en diensten te ontwikkelen volgens de principes van cyber security en privacy by design. Niet-C14-producten en -diensten mogen niet meer geïmporteerd, aangeboden en verhandeld worden in de C14-zone tenzij ze gecertificeerd zijn.
Een aantal multinationals als Intel, Microsoft, Google en Cisco hebben besloten de Convention regels te onderschrijven en verwerven zich daarmee een preferente positie op de C14-markt. Firma's zoals Apple, Brainbook, Philips, Huawei, eBay en de Nederlandse startup eVoting kiezen er bewust voor hun innovatie en productontwikkeling naar buiten de C14-zone te verplaatsen waar minder strikte veiligheidseisen gesteld worden aan ICT. Ook TomTom heeft aangekondigd dat zij de ontwikkeling van de TomTom-Scootmobiel naar de VS gaan overhevelen.

Het veel veiliger onder strikte governance zijnde Cyberspace betekent meer macht voor de cyber-multinationals die de Convention on Cybercrime van Den Haag onderschrijven doordat sprake is van een sterk door standaarden gedreven markt. De C14-landen hebben daarbij meer grip op hun cyberspace en in- en uitgaande informatiestromen. Hun vitale infrastructuur, bedrijven en burgers krijgen een veiliger cyberspace en meer garanties op privacybescherming.

5.4 Cyberconflict

Met de Haagse Convention proberen landen tegelijkertijd het risico op een cyberconflict te verkleinen. Uit een toespraak van de Nederlandse commandant van het Defensie Cyber Commando blijken echter zorgen: "Het besloten deel van Cyberspace zorgt ervoor dat mijn commando zich onvoldoende kan prepareren op cyberconflicten. Om voldoende kennis op te doen moeten we toegang hebben tot de rauwe, wildwest cyberspace-omgeving. Dat hebben we nu alleen in beperkte mate op Curaçao tot onze beschikking." De commandant ziet de toenemende eenvormigheid aan ICT-producten in Nederland, ook al zijn ze veiliger, met lede ogen aan. "We prepareren daarmee onze samenleving als slagveld voor een nieuwe cybertegenstander."
Grote landen betichten de C14 in VN-werkgroepen van protectionisme. Ook het weghalen van achterdeuren in ICT-producten ligt volgens hun diplomaten moeilijk. Politici uit de C14-landen denken dat die landen minder vat hebben op onze op ICT-gebaseerde infrastructuren voor e-spionage en voorbereidingen voor mogelijke cyberconflicten.

5.5 Internet governance

Onze overheid heeft als eerste de Haagse Convention on Cybercrime geratificeerd en voert de maatregelen tot op het scherpst van de snede door ondanks grote bedenkingen van een deel van het parlement. Waar heeft dit beste-jongetje-van-de-klas syndroom toe geleid na vijf jaar 'war'? Burgers moeten hun gehaalde e-rijbewijs tonen bij het verlengen van hun internetabonnement. Ook maakt het e-rijbewijs onderdeel uit van de integratietoets. Burgers kunnen zonder het overleggen van e-rijbewijs vanaf volgend jaar geen slimme koelkast, TV, oven of e-bike meer kopen. Die producten moeten voorzien zijn van een cyber- en privacy-veiligheidslabel. Alleen met een groot e-rijbewijs mag een burger nog een onveiliger klasse B product kopen dat zelf onderhouden moet worden. De burger is dan voor alle cyberschade en de gevolgen daarvan aansprakelijk; iets waarvoor hij/zij zich niet kan verzekeren. Burgers die na tien keer examen nog niet geslaagd zijn voor hun

e-rijbewijs mogen alleen een A+ klasse product kopen dat een sterk beperkte cyberfunctionaliteit kent en volautomatisch van patches voorzien wordt. ICT Nederland als lobbygroep wil dat Nederland massaal overgaat naar de nieuwe veiligheids-standaarden. Zowel grote ICT leveranciers als MKBers willen het voortouw nemen bij het op de markt brengen van veilige op ICT-gebaseerde producten. Voor het eerst wordt garantie gegeven op nieuwe software. Eis van de private partijen die vaart willen maken is wel dat Nederland uiterlijk eind dit jaar volledig overgaat naar IP versie 6 en DNSsec. IP versie 4 diensten moeten dan worden afgekoppeld. Het Parlement heeft de roep om zo'n maatregel onder druk van de *unplugged*-acties bekrachtigd in een motie. Er wordt doorgepakt: binnen twee maanden is er een breed publiek-privaat ondersteunde nieuwe nationale cyber security strategie. Nederland is daarmee internationaal voorloper binnen de C14-groep in het cyberveiliger maken van haar deel van cyberspace. De BOVAG pleit inmiddels voor een viermaandelijkse software-APK voor motorvoertuigen en het CBR stelt voor om het kunnen patchen van voertuigen op te nemen als bijzondere verrichting tijdens het rijexamen.

De nieuwe internationale ordening leidt tot een internationale tweedeling: een veilige cyberspace en het klassieke, ietwat anarchistische cyberspace met veel vrijheid, weinig controle en veiligheidsrisico-aspecten waarin de cybermaffia zelfs cyber-kapers-nesten weet op te richten. Vrijhandelsplaatsen zoals E-Goods for Freedom zijn sterk in opkomst. Voor het veilige Nederlandse cyberspace segment betekent dat het cyberrisico ineens verzekerbaar werd, iets dat u ook opgevallen moet zijn, gegeven de campagne "Even Apeldoorn twitteren." Nieuwe businessmodellen en bedrijven floreren inmiddels in het beschermende cyberspace gedeelte. Nieuwe burgerinitiatieven voor het afzweren van privacy-onveilige producten zoals klantkaarten blijken zeer succesvol. Nederland is daardoor in de afgelopen twee jaar snel een Secure Haven geworden voor privacy-minnende diensten en voor veilige, energie-neutrale dataopslag. Die ontwikkelingen lijken weer nieuwe internationale cyberdienstverleners aan te trekken die lange tijd snakten naar een veiliger cyberspace. Een vliegwiel. Uit peilingen van een erkend onderzoeksbureau blijkt dat het vertrouwen van onze burgers en het MKB in de cyberveiligheid van producten, de bescherming van privacy en de overheid als geheel het hoogste is sinds 1996.

5.6 Technologie adoptie

Tot zover het goede nieuws. Langzamerhand worden de negatieve aspecten van onze keuzerichting ook duidelijk. We hebben een *vendor lock-in*: de besloten markt zorgt voor duurdere producten en ICT-diensten. Zijn de door ICT-conglomoraten vastgestelde veiligheids- en privacystandaarden wel degene die we als maatschappij willen hebben? Zijn ze wel 'open' genoeg? Worden de ICT-werelden van het besloten deel en het open deel van cyberspace niet sterker door softwarefabrikanten uiteengedreven dan op grond van de verschillen in veiligheid verwacht mag worden?
Innovaties, denk aan IP versie 7 en allerlei Internet-of-All-Things producten komen pas veel later binnen de C14-landen beschikbaar omdat ze eerst door complexe en trage certificeringstrajecten heen moeten, als leveranciers ze al binnen de C14-zone willen leveren. Er zijn stringente controles door I&V-diensten en digitale politie op de koppelingen tussen de twee delen van Cyberspace. De douane-controles aan de grenzen van de C14-landen en hun cyberspace waarmee innovatieve apparaten, apps en software worden tegengehouden, leveren veel ergernis op van burgers. Buitenlandse bezoekers kunnen nog alleen via telefoon communiceren of moeten een e-wasstraatabonnement voor communicatie met het onveilige deel van cyberspace aanschaffen. Illegale import is moeizaam onder controle te houden.

De verplichte overgang naar veiliger producten valt slecht bij sommige in de C14 gevestigde multinationals. Moeten zij geheel of gedeeltelijk overstappen op veilig cyberspace, en hoe dan, of moeten ze zich uit de C14 terugtrekken? Het gaat hen veel te snel. Van innovatief voorop lopen als dé e-dienstverlener in de wereld zakt Nederland wellicht af tot een middelmoot; maar wel veilig.

Voor werkelijke ICT-innovatie moet je niet in de C14-zijn. Daarvoor moet je naar het veel minder gereguleerde deel van cyberspace. Gelukkig hoeven we daarvoor alleen naar België te rijden. Maar ook het gezondheidskostenbesparende e-ondergoed gaat aan ons voorbij. IJsland heeft daarmee de kosten voor de nationale gezondheidszorg kunnen halveren doordat ze nu vaak preventief kunnen ingrijpen. Bij ons lopen jaarlijks de gezondheids-zorgkosten op met zo'n vijf procent omdat onze privacyregels het gebruik van dergelijke ICT voorlopig verbieden. Een aantal andere voorbeelden worden aan het begin van dit artikel genoemd.

Kortweg een situatie van cyberstroop: het smaakt geweldig en levert veilige stroopwafels, maar we lopen oubollig achter op ten opzicht van onze buren en andere landen. Aan ons samen, burgers, publiek-privaat, overheid en regelgever de keuze welke richting we moeten kiezen: rechtlijnig door of toch af en toe een hap van een 'onveilige' stroopwafel? Uw reacties: #stroopwafel of nrcyb@nrc.nl.

5.7 Indicatoren

Economie

Indicator		Assessment
Vestigingsklimaat		Positief voor cyber securitymarkt
		Negatief voor deel innovatieindustrie
Open / gesloten		"Cyber Schengen" - binnen open, gesloten voor buiten
Duurzaamheid		Mogelijk neveneffect
Groei		Securitymarkt sterk gestimuleerd; nieuwe diensten
		Deel innovatiemarkt trekt weg
Arbeidsmarkt		Positief voor nieuwe ICT security&privacymarkt
		Negatief voor deel innovatieindustrie
Sociaal maatschappelijk		Burgers worden beperkt in ICT-keuzes
		Sterkere controle op ICT-keuze en gebruik Onthouden van nieuwe (gezondheids)middelen
		Minder cyberonveiligheid

Veiligheid

Indicator		Assessment
Economisch		Ongebreidelde innovatie geremd
		Sommige innovatie niet beschikbaar voor Nederland
		Stimulatie Cyber security en privacy-by-design; veilige producten en diensten
		Nieuwe diensten (Safe Haven)
Aantal/aard incidenten		Afgenomen op de aspecten privacy, security en safety
Gevoel		Vertrouwen in veiligheid producten en diensten sterk gestegen
		Vertrouwen in overheid sterk gestegen
Bewustwording		Impliciete veiligheid; geen aandacht
Mogelijkheden		Cyber security en privacy-by-design
		Cyberverzekeringen
		Softwaregaranties
		Operationele kanttekeningen Cyber Commando

Privacy / vrijheid

Indicator		Assessment
Bewustwording		Hoog door cyberincidenten en grootschalige ID fraude
Schendingen		Aanleiding: Grootschalige ID fraude & crime
		Onder controle
Technologie		Io(A)T en andere ICT innovatie wordt vertraagd
		Cyber security en privacy-by-design
Mogelijkheden		Eisen, regelgeving en afgedwongen standaarden
		Tweedeling Cyberspace geeft barrières

5.8 Tot slot

Dilemma's

- Protectionisme in samenspraak met een blok aan landen en private partijen versus open markt en globalisering.
- Publiek-privaat doorpakken op security en privacy by design versus optimisme dat de markt het uiteindelijk oplost (doorpakken versus polderen, pappen en nathouden).
- Innovatiesnelheid versus vrijheid en veiligheid/ privacy.
- Sectortoezichthouders houden verplicht toezicht op ICT security, safety en privacy versus alleen toezicht op de klassieke sectorfuncties.

Stakeholders

- ICT multinationals en grote ICT-conglomeraten.
- MKB.
- Burgers.
- Publiek-Private vitale infrastructuren.
- Gelijkgestemde landen.
- Overheidspartijen (EZ, SZ&W, VenJ, Defensie, BZ).
- Cybercriminelen en actoren van vreemde staten.

Kansen

- Security, safety en privacy als economische motor.
- Cyber security en privacy-veiligheidslabels op alle producten met ICT.
- Tot stand brengen van de Europese CyberAutoriteit (ECA) (root cause analyse ernstige incidenten; aanwijzingen voor de industrie).
- Veilige ICT producten voor 'dummies'.
- Snelle invoering IPv6 en DNSSec.

Bijlage 1

Het analistennetwerk Nationale Veiligheid

Het Analistennetwerk Nationale Veiligheid (ANV) is een gezaghebbend kennisnetwerk dat sinds 2011 jaarlijks de NRB opstelt, in opdracht van het ministerie van Veiligheid en Justitie namens de Stuurgroep Nationale Veiligheid (SNV).
Tot en met 2010 lag de verantwoordelijkheid voor de NRB bij een aantal departementen, waarbij het ministerie van Veiligheid en Justitie als coördinator optrad. De SNV heeft geconstateerd dat – om de continuïteit, borging van de kennis en de multidisciplinaire aanpak te versterken – het gewenst is deze rol te beleggen bij kennisinstellingen. Ontwikkeling en onderhoud van kennis is immers core business van dit soort organisaties. Omdat nationale veiligheid een breed terrein bestrijkt, met vele disciplines, is het plan opgevat deze organisaties in een netwerkstructuur te laten opereren. Dit plan heeft geleid tot de vorming van het ANV.

Het ANV bestaat uit een vaste kern van zes organisaties (de **Taakgroep NRB**) en daaromheen een netwerk (de Ring) van kennisinstellingen, diensten, bedrijven en onderzoeksbureaus die afhankelijk van de kennisvraag worden ingeschakeld bij de productie van de NRB. De vaste kern wordt gevormd door de volgende zes organisaties:

- Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
- Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Veiligheid en Justitie
- De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
- De Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO
- De Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael'
- Het Institute of Social Studies (ISS) van de Erasmus Universiteit Rotterdam

Deze organisaties beschikken over brede, multidisciplinaire expertise en bestrijken daarmee gezamenlijk het werkveld van de Nationale Veiligheid. Op deze wijze is de *All Hazard benadering* voor de NRB gegarandeerd en is de eenheid in methodologie en overkoepelende analyses geborgd.

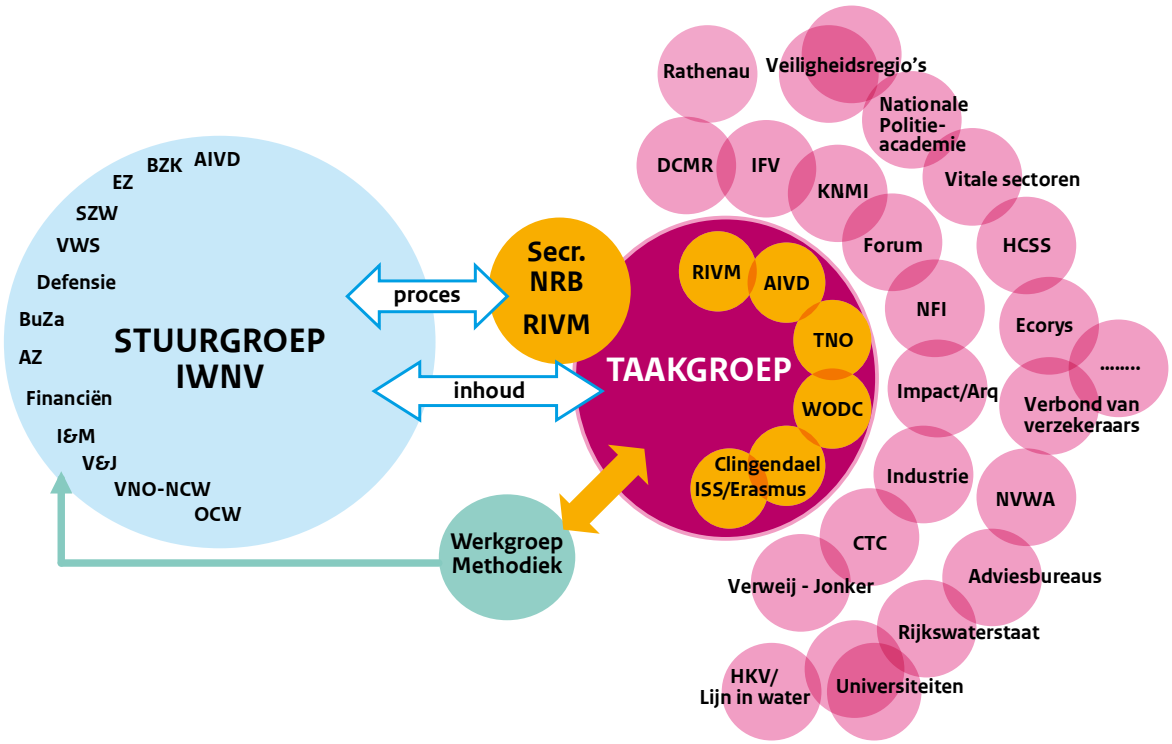
De zes instellingen in de kern dragen gezamenlijk de verantwoordelijkheid voor de inhoudelijke kwaliteit van de NRB. Specifieke, aanvullende expertise wordt geleverd door de andere organisaties in het netwerk. De organisaties in de kern en de ring stellen experts en analisten ter beschikking, die in (in samenstelling steeds wisselende) werkgroepen inhoudelijke activiteiten uitvoeren voor de NRB. Een ondersteu-

nend secretariaat (het **NRB secretariaat**) bestaande uit een algemeen secretaris, werkgroepcoördinatoren en projectondersteuning draagt zorg voor de processturing, voortgangsbewaking en ondersteuning van het tot stand brengen van de NRB. Het NRB secretariaat is het vaste aanspreekpunt voor de SNV, de IWNV (Interdepartementale Werkgroep Nationale Veiligheid) en de aangesloten departementen. Verder ondersteunt het NRB secretariaat de Taakgroep en de scenariowerkgroepen bij de productie van de NRB en stuurt en bewaakt zij het proces. Het NRB secretariaat is gevestigd bij het RIVM.

De taken van het ANV zijn:

1. Het produceren van de jaarlijkse Nationale Risicobeoordeling, waarbij de SNV bepaalt welke thema's in de NRB dienen te worden uitgewerkt.
2. Het (jaarlijks) adviseren van de SNV over de relevante thema's voor de (volgende) NRB, waarbij naast incidentscenario's ook ontwikkelingen op de (middel)lange termijn en sluipende processen worden meegenomen.
3. Het uitvoeren van thematische verkenningen, ad hoc analyses en andere studies op het gebied van Nationale Veiligheid.

Figuur 3. Schematische weergave van de organisatiestructuur van het Analistennetwerk Nationale Veiligheid



Bijlage 2

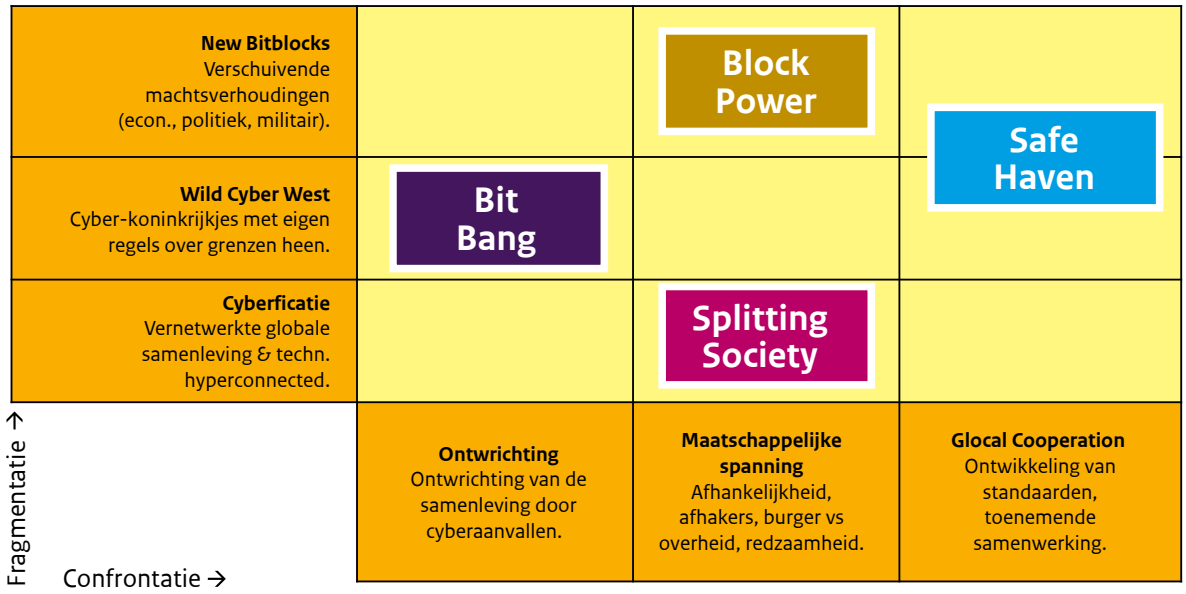
Scenariomethodiek

De gehanteerde scenario-methodiek is gebaseerd op het orthogonaal kruisen van twee factoren die uit de voorafgaande brainstorm zijn gekomen als belangrijke ontwikkelingen met een onzekere uitkomst met een hoge impact. Het zijn de factoren fragmentatie en confrontatie.

Per factor zijn drie verschillende gezichtspunten gedefinieerd. Het zijn op zichzelf staande gezichtspunten met eigen karakteristieken. De twee factoren met elk drie gezichtspunten geven een stelsel van mogelijke toekomstscenario's.

Uit dit stelsel is een viertal scenario's geselecteerd waarmee een breed spectrum van plausibele toekomsten is gecreëerd.

Figuur 4. Tabel met daarin de vier blokken van de scenario's.



Bijlage 3

Brainstorm Cyber ontwikkelingen

Aan de brainstormbijeenkomst, gehouden op vrijdagmiddag 4 september bij TNO in Den Haag, nam een breed spectrum aan experts op het gebied van cybersecurity deel. Deze bijeenkomst diende als voorbereiding op de Challenge week waarin de cybersecurity toekomstscenario's geschreven dienden te worden. Doel was om de schrijvers van input te kunnen voorzien, maar ook om hen bewust te maken van de verscheidenheid aan gezichtspunten rondom dit thema.

Proces

Er waren 29 aanwezigen, waaronder de organisatoren vanuit TNO en het ANV. Een deelnemerslijst is achteraan deze bijlage toegevoegd.
De aanwezigen zijn in vier groepen verdeeld, waarbij aan elke groep één van de schrijvers was toegevoegd. Op deze wijze werden de schrijvers met informatie vanuit de groep gevoed.
Er is in drie rondes gediscussieerd. De eerste ronde om in kaart te brengen wat er nu speelt op cybergebied. De tweede ronde diende om de ontwikkelingen in de nabije toekomst van 2022 te schetsen. De derde ronde om een beeld te krijgen van mogelijke cyberontwikkelingen omstreeks 2030. Elke ronde vond eerst plaats in groepsverband, waarna in een plenaire sessie de hoofdpunten besproken werden. Deze punten zijn gedocumenteerd onder de vier thema's Adoptie van nieuwe technologie, Internet governance, Staatsmacht en Cyberconflict.

Uitkomsten

2015 – Adoptie van nieuwe technologie

- Nederland is een voorloper mbt adoptie van internettechnologie.
- Internet of Things (IoT) is in opkomst, de eerste toepassingen zijn er.
- Data explosie is begonnen (reclame, gezondheid, verzamelen persoonlijke data).
- Veel oude technologie aangesloten op internet die daar niet voor ontwikkeld was. Legacy systemen die met patches bijgewerkt worden.
- Big data tech met predictive analytics groeit in mogelijkheden.

2015 – Internet governance

- Er heerst een onmacht om te reguleren. Overheden lopen structureel achter mbt governance.
- Het internet (en data) is relatief ongereguleerd. Geen duidelijke aansprakelijkheid op dit moment omtrent bijvoorbeeld de bescherming van consumentendata.
- Het huidige beleid holt achter de technologie aan en kenmerkt zicht door pleisters plakken ipv een paradigma-shift die nodig is om wet en regelgeving up-to-date te krijgen met de digitale tijd. Problemen onttrekken zich daardoor aan het zicht wat niet bevordelijk is voor het risicobesef.
- Verschilldende visies vanuit verschillende departementen.
- Steeds grotere data-breaches, maar wat wordt uiteindelijk de game changer voor vertrouwen (dat er nu nog is)?
- Er is een gebrek aan visie op privacy issues
- Wat is het verdienmodel van alle publieke data richting de maatschappij?

2015 – Staatsmacht

- Follow the Money wordt steeds meer Follow the Data.
- Er is behoefte aan reflectie, het ontbreekt aan een professionele visie op de kansen, bedreigingen maar vooral ook de complexiteit (hoge verbondenheid van alles en iedereen) van het cyberdomein.
- Onduidelijkheid/strijd beleggen verantwoordelijkheid bij burger/bedrijfsleven/overheid.
- Ethische vraagstuk: hoe zit het met de bescherming van digitaal kwetsbare groepen? Worden nu aan hun lot overgelaten?
- NL digitaal platgelegd nadat Rusland voor het Internationaal Strafhof gedaagd werd vanwege MH17.
- Wat is plan B als het internet niet werkt en we weten niet waarom?
- De gebruiker als zwakke schakel (Snowden) die een heleboel kan breken.
- Het lijkt sociaal geaccepteerd om van niks te weten als het op cyber- en data security aankomt.

2015 – Cyberconflict

- Er zijn zowel state-actors als private actoren. Er is dus geen dominante staatsmonopolie op geweld zoals daar bij fysiek geweld sprake van is.
- Democratisering van cybercrime. Cybercrime as a service, je kunt hackers eenvoudig inhuren, ook als prive persoon.
- Er ontstaat een nieuwe ruimte waar inter-statelijke conflicten uitgevochten kunnen worden.
- Balkanisering van het internet: het valt uiteen in grote en kleine partijen die niet noodzakelijk een staat vertegenwoordigen. Versplinterd.
- Cryptogafie werkt nu nog maar quantum computing kan hier verandering in gaan brengen.
- Cyberconflicten kunnen in toenemende mate consequenties in de fysieke wereld hebben (platleggen specificieke faciliteiten).
- Cybersecurity is een dreiging die door angst is gedreven, niet evidence driven.
- Vertrouwen speelt een belangrijke rol.
- Militarisering van het internet. State-sponsored espionage.

2022 – Adoptie van nieuwe technologie

- Het internet gaat van gedistribueerd netwerk naar een paar ethernetkabels van grote providers via internet exchanges.
- Onmogelijkheid om data nog te beschermen door onbetrouwbare software.
- Data met steeds meer samenhangende algorithmen die bepalend worden (semantic web technologie). Hoger gebruik van producten, maar minder bezit van producten.
- Er zal een offline beweging ontstaan die niet meer deelneemt.
- Welke banen staan nog overeind?
- Wel/niet quantum-resistant crypto.
- Verzekeringen op basis van big data betekenen het einde van het sociale verzekeringsstelsel.
- Trouwen met robots.
- E-health neemt een vlucht en maakt de huisarts steeds meer overbodig. Toenemende customization van diensten (ehealth, onderwijs etc.).

2022 – Internet governance

- Beleid onstaat om het aantal dodelijke slachtoffers door cyber terug te dringen.
- Commercialisatie van cyberdiensten.

- Vertrouwen: regulering remt de innovatie maar noodzakelijk om aansprakelijkheid en verantwoordelijkheid te regelen.
- Verlies van elementaire rechtsbescherming van individuen door onwil om aansprakelijkheid toe te wijzen: recht van de sterkste met de meeste data.
- Twee internetten: openbaar deel en een gesloten deel.
- Ministerie van Internet is een feit.
- De overheid zal actiever moeten worden (analogie: opkomst auto en uiteindelijk verkeersregels en stoplichten).
- Komt er een verzekeringsgedachte a la systeembanken? Wordt cyber een NUTS voorziening?

2022 – Staatsmacht
- Partijen als Facebook hebben steeds meer macht, concentreert zicht ook.
  - Deze zijn echter ook kwetsbaar doordat gebruikers kunnen opstaan en weglopen.
- China is dominant (is ook hun doelstelling).
- Vertrouwen van burgers/consumenten heeft een tik gehad door data verlies en de schade die dat berokkend (identiteits diefstal).
- Banken zijn gebroken en weg (geld kan steeds makkelijker verplaatst worden of vervangen (bitcoins)).
- Voortgaande flexibilisering van werk en organisatie.
- Algoritmen worden bepalender in ons leven.
- Twee nu grote internetbedrijven zijn weggevaagd omdat ze cybersecurity niet serieus hebben genomen. Andere bedrijven zullen juist steeds meer macht naar zich toegetrokken hebben door producten en diensten via hun portals te laten lopen.

2022 – Cyberconflict
- Cyberaanslagen zijn een feit.
- Cyberconflict kan tot een Artikel 5 procedure van de NATO leiden.
- Cybergijzeling.
- Er komen proliferatieverdragen voor Digitale wapens.
- Cyberwapenwedloop.
- Rode cybertelefoon (die dan ook niet gehackt wordt).
- Cyberwar afdeling van het leger, ontstaan nieuwe mogelijkheden van oorlogvoering.

2030 – Adoptie van nieuwe technologie
- Verlies van autonomie door afhankelijkheid van cyber / je data-bestaan.
- Data-gedreven ontwerp wordt dominanter.
- Ethiek wordt gecodeerd.
- Er zijn bewuste digitale afhakers.
- Werk ziet er anders uit door de verregaande digitalisering. Kan iedereen dit bij benen?
- Stukken van de overheid worden geheel gedigitaliseerd.
- Van digitale naar biochemische communicatiesystemen en daarmee de integratie van de mens in het systeem.
- Smartphones als implantaat.

2030 – Internet governance
- Nederland/de EU heeft een voorbeeldfunctie over de regulering en eisen die aan bedrijven op cyber- en datagebied gesteld worden.
- Internet in brokken (dark web).
- Stukken van de overheid worden geheel gedigitaliseerd.
- Door afbreuk fundamentele rechtsbescherming is privacy als individueel en maatschappelijk belang volledig erkend en wordt dit maatschappelijk beschermd.

2030 – Staatsmacht
- Complexiteit van het cybersysteem (netwerkeffecten van alles dat verbonden is) en de aangrijping daarvan op de fysieke wereld maken disruptie makkelijker, maar kan mogelijk ook back-firen? Vergelijk de huidige macht van de financiele sector/banken door onoverzichtelijke complexiteit (aanklacht Joris Luijendijk).
- Strijd om data beheersing bepaald wie macht heeft.
- Ontwikkeling van algoritmen in openheid om de veiligheid en betrokkenheid te vergroten.
- NL als voorbeeld in 2030: Een land waar je zeker weet dat je data veilig is. Vertrouwen als businessmodel.

2030 – Cyberconflict
- Grote storingen op de cyberinfrastructuur ontwrichten de maatschappij.
- Autonome digitale wapensystemen.

Samenvattend
- Tussen hoop een vrees: Vertrouwen speelt een grote rol tegen de achtergrond van de gevoerde discussies in adoptie van technologie (beleving vs rationaliteit). De ethische aspecten van cybertechnologie lopen nog sterk achter.
- Complexiteit van het gehele systeem.
- Determinisme (cyber ontwikkeld zich vrij) vs Instrumentalisme (regulering, richtinggevend, Internet als NUTS voorziening).

Deelnemers

Naam	Organisatie	Rol
Allard Kernkamp	TNO	schrijver
Hans Stavleu	TNO	methodiek begeleider
Eric Luiijf	TNO	schrijver
Rinke Klein Entink	TNO	methodiek begeleider
Douwe Bierma	TNO	projectcoördinator
Marcel Mennen	RIVM	Alg secr Analistennetwerk
Sico van der Meer	Clingendael	schrijver
Frans-Paul van der Putten	Clingendael	expert
Cyber expert	Inlichtingendiensten	expert
Cyber expert	Inlichtingendiensten	expert
Jelle van Haaster	Defensie Academie/Faculteit Militaire Wetenschappen	expert
Mieke van Heeswijk	SIDN fonds	expert
Sergei Boeke	Universiteit Leiden, CTC	expert
Christian Doerr	TU Delft	expert
Ben van Lier	Directeur strategie en innovatie CENTRIC	expert
Bert Mulder	Haagse Hogeschool en e-society instituut	expert
Dennis Broeders	Wetenschappelijke Raad voor het Regeringsbeleid	expert
Geert Munnichs	Rathenau instituut	expert
Maarten Gehem	HCSS	schrijver
Ronald Prins	Fox-IT	expert
Prof. dr. B. Jacobs	Radboud Universiteit, Hoogleraar computerbeveiliging	expert
Chris van ‘t Hof	Tek Tok, presentator en schrijver	expert
Melanie Riebeck	Radically open security	expert
Michiel Steltman	DINL	expert
Jeroen van der Ham	NCSC	expert
Diederik van Luijk	NCSC	expert
Analist	NCTV	expert
Frank Breedijk	Schuberg Phillis	expert
Bas Straathof	Centraal Plan Bureau	expert

Toekomstverkenning: Het cyberdomein in 2022
Allard Kernkamp (TNO)
Sico van der Meer (Instituut Clingendael)
Eric Luiijf (TNO)
Maarten Gehem (HCSS)
Marcel Mennen (RIVM, editor)
Contact: douwe.bierma@tno.nl

Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Dit is een uitgave van:

**Rijksinstituut voor Volksgezondheid
en Milieu (RIVM)**

**Wetenschappelijk Onderzoek- en
Documentatiecentrum (WODC)**

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)

**Nederlandse Organisatie voor toegepast-
natuurwetenschappelijk onderzoek TNO**

**Stichting Nederlands Instituut voor
Internationale Betrekkingen 'Clingendael'**

**Erasmus Universiteit Rotterdam,
Institute of Social Studies (ISS)**

Postbus 1 | 3720 BA Bilthoven
www.rivm.nl

December 2015

De zorg voor morgen
begint vandaag