www.pwc.nl

Verkenning naar gescheiden ICT-netwerken en -diensten in Nederland

September 2014

2014-1319/OV/ww/mp

pwc

Inhoudsopgave

PwC heeft dit rapport opgesteld op basis van de opdrachtbevestiging van NCTV van 30 juni 2014, met kenmerk 40100008694, waarin gerefereerd wordt aan onze offerte van 20 juni 2014, met kenmerk 2014-0722/OV/ww/mp. PwC heeft hierbij tevens rekening gehouden met de discussies die hebben plaatsgevonden in bilaterale gesprekken tussen NCTV en PwC, in interviews met leden van de stuurgroep, en in een drietal werksessies met overige betrokkenen. Deze gesprekken hebben geleid tot beperkte aanpassingen van de scope, in die zin dat het verkennende karakter van de studie benadrukt is. Het onderzoek is uitgevoerd in de periode 23 juni 2014 tot en met 19 augustus 2014. PwC aanvaardt geen aansprakelijkheid of verantwoordelijkheid jegens enige partij met betrekking tot de inhoud van dit document.

Samenvatting

De Nederlandse samenleving loopt steeds meer risico als gevolg van cybersecurity dreigingen, zoals ook geschetst wordt in het Cybersecuritybeeld Nederland 4[1]. Naarmate het belang en de waarde van de digitale component in de samenleving toenemen, wordt de mogelijke impact van dergelijke risico's op de digitale veiligheid van individuen, bedrijven en overheden groter. Recente onderzoeken schatten de economische schade van cybercrime in Nederland op 8,8 miljard euro per jaar[2]. In Nederland hebben incidenten, de DDoS-aanvallen die in 2013 diverse websites van de overheid en enkele banken tijdelijk onbereikbaar maakten, en de onthullingen van Edward Snowden over spionage door buitenlandse mogendheden, aanleiding gegeven tot debat. Naar aanleiding van de DDoS-aanvallen, is in de *Nationale Cyber Security Strategie 2,* door de minister van Veiligheid en Justitie het volgende toegezegd:

"Er wordt een verkenning uitgevoerd in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. Met een gescheiden netwerk nemen de mogelijkheden om de continuïteit van vitale processen te borgen toe. Ook kunnen binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld. Hierdoor kan de privacy/integriteit van de data in deze opslag of cloud worden verbeterd"

PwC heeft op verzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid een verkennend onderzoek uitgevoerd naar de vraag: *zijn gescheiden ICT-netwerken in Nederland* ***haalbaar*** *en* ***wenselijk****?*

De voorliggende rapportage bevat de resultaten van deze verkenning. De resultaten beschrijven in eerste instantie het theoretische kader dat gehanteerd wordt. Vervolgens worden buitenlandse en Nederlandse voorbeelden en ontwikkelingen omtrent gescheiden netwerken beschreven. Ten slotte wordt een antwoord gegeven op de vraag of gescheiden ICT-netwerken in Nederland haalbaar en wenselijk zijn.

Cybersecurity vereist een balans tussen belang, dreiging, weerstand en beschikbare middelen

In de discussie over cybersecurity is het zinvol veiligheid van ICT-netwerken te duiden aan de hand van drie aspecten: ***beschikbaarheid***, dat betrekking heeft op de mogelijkheid gebruik te maken van de dienst op de afgesproken tijden, waarbij aspecten als tijdigheid, continuïteit en robuustheid een rol spelen, ***integriteit***, dat betrekking heeft op de juistheid en volledigheid van de data, en ***vertrouwelijkheid***, dat betrekking heeft op de exclusiviteit van de data en van de toegang daartoe.

Cybersecurity is gericht op het beschermen tegen risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van ICT-infrastructuren en gegevensverwerkingen. De noodzaak en wenselijkheid van te treffen beveiligingsmaatregelen hangt hierbij enerzijds samen met het belang van de ICT-infrastructuren en gegevensverwerkingen, en anderzijds met de (gepercipieerde) bedreigingen en de resulterende risico's voor de veiligheid daarvan. Uit het *Cybersecuritybeeld Nederland 4* komt naar voren dat staten en cybercriminelen op dit moment de grootste dreiging vormen voor de beschikbaarheid, vertrouwelijkheid en integriteit van Nederlandse ICT-infrastructuur. Afhankelijk van de specifieke toepassing (bijvoorbeeld elektriciteitsvoorziening of het bieden van gezondheidszorg) zoekt men een balans tussen het belang (beschikbaarheid, integriteit en/of vertrouwelijkheid), de dreiging en de weerstand tegen deze dreigingen, én de hoogte van de benodigde inzet van middelen om deze te waarborgen.

[1] Beleidsreactie Cybersecuritybeeld Nederland 4, 10 juli 2014.

[2] Kamerbrief inzake Beantwoording Kamervragen over bericht dat cybercrime Nederland jaarlijks 8,8 miljard euro kost, d.d. 13 augustus 2014. Deze schade is echter moeilijk vast te stellen, en het bedrag kan dan ook moeilijk gestaafd worden.

Een 'volledig gescheiden ICT-netwerk' is een ICT-netwerk dat vanuit alle perspectieven tot op elk niveau gescheiden is

In de *Nationale Cyber Security Strategie 2* wordt gesproken over gescheiden ICT-netwerken voor publieke en private vitale processen. In dit rapport wordt kortweg de term *gescheiden ICT-netwerken*, of *gescheiden netwerken* gebruikt. Met ICT-netwerken doelt men op het geheel van apparaten die door middel van kabel- of draadloze verbindingen, via routers die het dataverkeer sturen, in verbinding staan met andere apparaten en ICT-diensten (waaronder clouddiensten). Wij introduceren drie perspectieven waarlangs men ICT-netwerken kan scheiden:

1. **Productieketen:** de productieketen loopt van het ontwerp van de componenten, tot het beheer en gebruik van de ICT-infrastructuur. De bouw, de exploitatie en het onderhoud van een (eventueel gescheiden) ICT-netwerk gebeuren in de context van een internationale productieketen. Een deel van de kwetsbaarheden in ICT-netwerken vindt zijn oorsprong in de keten van ontwerp en bouw van netwerkcomponenten tot upgrades van het netwerk: welke kwetsbaarheden zijn, al dan niet bewust, in componenten ingebouwd? Een ander deel van de kwetsbaarheden in ICT-netwerken komt voort uit het beheer en onderhoud van het netwerk: wie hebben toegang tot een netwerk via beheer en onderhoud, en met welke intenties? Bij het eventueel scheiden van ICT-netwerken dient dus rekening te worden gehouden met deze ketenrisico's.
2. **Netwerkhiërachie:** ten tweede kan gekeken worden naar de mate waarin de scheiding wordt doorgetrokken door de verschillende hiërarchische niveaus van het netwerk, die lopen van de gebruiker en zijn/haar terminal (zoals PC, laptop, tablet of smartphone), via het toegangsnetwerk en het kernnetwerk, naar de applicaties, dienstplatformen of cloud. Op elk van deze niveaus kan al dan niet sprake zijn van gescheiden infrastructuur of gescheiden toegang. In bestaande voorbeelden van gescheiden ICT-netwerken is er vaak slechts sprake van scheiding in één of een aantal van deze niveaus. In een dergelijk geval is er sprake van gedeeltelijke scheiding. Een verdere scheiding van ICT-netwerken vereist in veel gevallen een aanzienlijk grotere inzet van middelen.
3. **Fysieke versus virtuele scheiding:** een aanvullend perspectief op een ICT-netwerk volgt uit het OSI-model, een door de *International Organization for Standardization* (ISO) gestandaardiseerd referentiemodel voor datacommunicatie dat in sterk vereenvoudigde vorm bestaat uit drie lagen: de fysieke laag, de capaciteitslaag en de virtuele laag[3]. Elke laag voegt hierbij functionaliteit toe, zodat het mogelijk wordt gemaakt dat fysieke signalen uiteindelijk de vorm krijgen van voor eindgebruikers begrijpelijke informatie zoals tekst en getallen. Anders dan bij het perspectief van netwerkhiërarchie wordt in het OSI-model dus een onderscheid gemaakt op basis van functionaliteit in plaats van op basis hiërarchisch niveau. De meest verregaande vorm van scheiding, het fysiek scheiden van een netwerk, vereist daarbij de grootste inzet van middelen. Er is een combinatie van fysieke scheiding, capaciteitsscheiding en virtuele scheiding - aangevuld met encryptie nodig - om een breed scala aan cybersecurity risico's te kunnen mitigeren. Fysieke versus virtuele scheiding kan plaatsvinden op verschillende niveaus van de hiervoor benoemde de netwerkhiërarchie.

De hiervoor beschreven drie perspectieven op een gescheiden ICT-netwerk tonen dat netwerkscheiding langs een glijdende schaal verloopt. De term gescheiden ICT-netwerk zal dan ook door verschillende betrokkenen verschillend geduid worden. Een *volledig gescheiden netwerk* definiëren we hier echter als een ICT-netwerk dat langs alle drie perspectieven tot op elk niveau gescheiden is. Een dergelijke scheiding vereist een substantiële aanwending van middelen.

Een aanvullend perspectief op netwerkscheiding is *geografische scheiding*, wat impliceert dat bepaalde vitale processen en data geografische grenzen, zoals de landsgrenzen, niet mogen of zelfs kunnen verlaten. Dit kan bijvoorbeeld nodig zijn om te vermijden dat buitenlandse mogendheden toegang kunnen krijgen tot vertrouwelijke informatie.

In de praktijk blijkt geografische scheiding niet altijd mogelijk. Voor sommige diensten is toegang vanuit het buitenland juist een essentieel onderdeel. Bovendien komt informatie van het Internet via verschillende internationale routes op de plaats van bestemming. Bij clouddiensten kan een

[3] Gebaseerd op een vereenvoudiging van het 7-laags Open Systems Interconnect (OSI) model.

individueel databestand zich in stukken verdeeld op geografische locaties in meerdere landen bevinden. Hierop zijn meerdere nationale en internationale wetten van toepassing. Het is wel mogelijk om Nederlandse data te hosten in één of meerdere clouddatacenters op Nederlands grondgebied.

Dit betekent echter niet dat deze data ook *juridisch gescheiden* is van buitenlandse jurisdictie. Hiervoor zou moeten worden gewaarborgd dat data Nederlands grondgebied niet verlaat, en bovendien moet rekening worden gehouden met de eventuele extraterritoriale werking van wetgeving waar bedrijven onder kunnen vallen.

Een discussie over veiligheid van ICT-netwerken speelt ook in het buitenland, waar wordt ingezet op samenhangende pakketten aan cybersecuritymaatregelen

De discussie over de veiligheid van ICT-netwerken speelt in meerdere landen. Daarbij nemen de landen[4] uiteenlopende standpunten in wat betreft de te nemen maatregelen om cyberdreigingen te mitigeren. Deze standpunten lopen uiteen van het stellen van eisen aan dataopslag en -verwerking in het buitenland en het zelf aanleggen van eigen onderzeese kabels, tot het oprichten van publiek-private consortia om cybersecurity kennis te delen. In slechts een beperkt aantal van de beschouwde landen, waaronder Duitsland, wordt op vergelijkbare wijze als in Nederland gesproken over de opzet van een gescheiden ICT-netwerk. De internationale discussie over gescheiden netwerken lijkt dan ook in 2013 verder aangejaagd te zijn door de Duitse Bondskanselier, die pleitte voor een Europees Internet. De ontwikkelingen in het buitenland laten zien dat landen als het Verenigd Koninkrijk, Canada en Brazilië investeren in pakketten aan cybersecuritymaatregelen in plaats van zich op één oplossing te richten.

In Nederland bestaan diverse voorbeelden van deels gescheiden ICT-netwerken

Er bestaan in Nederland nu al verschillende ICT-netwerken die deels gescheiden zijn, zoals het C2000-netwerk, het Netherlands Armed Forces Integrated Network (NAFIN), het glasvezelnetwerk van Rijkswaterstaat, het GSM-Rail netwerk van ProRail, of het CDMA-netwerk dat Alliander bouwt voor het aansluiten van smart meters. Op dit moment is het programma Rijksoverheidnetwerk 2.0 (RON2.0) gestart waarbij de realisatie van een rijksoverheidsnetwerk samen met de consolidatie van datacenters dient als basis voor de Rijkscloud. In bepaalde vitale sectoren, zoals de financiële sector of de energiesector zijn bovendien zonder overheidsinterventie deels gescheiden netwerken aangelegd.

De bestaande gescheiden netwerken zijn op verschillende niveaus in productieketen, netwerkhiërarchie, of op fysieke of virtuele wijze, gescheiden als voortvloeisel van verschillende afwegingen op het gebied van technische interoperabiliteit, functionaliteit, veiligheid, kosten, en wetgeving. Bij geen van de bovengenoemde gescheiden ICT-netwerken is sprake van een volledige scheiding. Er zijn wel voorbeelden van netwerken die langs enkele van de beschreven perspectieven voor netwerkscheiding zijn afgezonderd, zoals het C2000-netwerk dat voor wat betreft het radionetwerk als een fysiek gescheiden netwerk beschouwd kan worden. Het maakt immers gebruik van een specifiek hiervoor aangelegd antennenetwerk, en van gereserveerde radiofrequenties.

De haalbaarheid van een volledig gescheiden ICT-netwerk is zeer twijfelachtig

Er is op dit moment geen volledig gescheiden netwerk in Nederland. Dit kan aanleiding geven tot de wens om voor specifieke diensten een volledig gescheiden ICT-netwerk aan te leggen, dat langs alle genoemde perspectieven volledig gescheiden is. In geen van de in dit rapport besproken voorbeelden is daar echter sprake van. Ook scheiding langs één van de genoemde perspectieven is niet eenvoudig.

[4] PwC heeft in deze analyse geen volledigheid nagestreefd, maar een beperkt aantal landen beschouwd.

Hiervoor zijn diverse redenen, waaronder:

- **Hoge kosten**: een volledig gescheiden ICT-netwerk, langs alle hiërarchische niveaus, waarbij gebruik gemaakt wordt van een volledig vertrouwde productieketen, zal erg kostbaar zijn.
- **Beperktere functionaliteit**: een volledig gescheiden ICT-netwerk impliceert dat er geen koppelingen zijn naar andere, mogelijk onveilige netwerken. Het succes van het Internet illustreert echter de meerwaarde die ontstaat door netwerkkoppelingen. De openheid van het internet heeft geleid tot snelle innovatie, een grote variëteit aan diensten, en de mogelijkheid om infrastructuurnetwerken tegen lage kosten van afstand te monitoren en onderhouden.
- **Gebrek aan voldoende kennis**: een organisatie die gebruikmaakt van een volledig gescheiden ICT-netwerk, zonder een beroep te doen op externe leveranciers, zal veel eigen ICT-kennis in huis moeten hebben. Met name het volledig vervangen van de internationaal verweven productieketen is niet realistisch.
- **Schijnveiligheid**: het in eigen huis bouwen, beheren en huisvesten van een ICT-netwerk hoeft niet per se te betekenen dat het netwerk veiliger is. Het kan zelfs een schijnveiligheid creëren, waarbij het idee ontstaat dat, doordat alles in eigen beheer is, het veiliger is. Bovendien ontstaat er een sterke afhankelijkheid van een enkel netwerk, indien een gescheiden ICT-netwerk wordt gebruikt voor het leveren van meerdere, eventueel vitale, diensten. Dat op zich kan de impact van veiligheidsrisico's vergroten, en creëert mogelijk een aantrekkelijk doelwit.

Bovenstaande redenen ten aanzien van de (on-)haalbaarheid dienen echter in relatie tot de potentiële baten (wenselijkheid) van een gescheiden ICT-netwerk bezien te worden. Deze zijn alleen per vitale sector, proces, product of dienst te bepalen. Hierbij dienen bovengenoemde generieke redenen voor de onhaalbaarheid van een gescheiden ICT-netwerk overigens ook aangevuld te worden met sector-, proces-, product-, of dienstspecifieke redenen.

Het kan echter wel haalbaar zijn om ICT-netwerken *deels* te scheiden op onderdelen van de drie perspectieven productieketen, netwerkhiërarchie en fysieke versus virtuele scheiding. De manier waarop hangt af van de dreiging waartegen bescherming is gewenst, en de mate waarin middelen beschikbaar zijn. De beheerder van een netwerk kan bijvoorbeeld de dreiging op aftappen verkleinen door netwerken fysiek te scheiden en de toegang ertoe geografisch te beperken.

Volledige scheiding van alle ICT-netwerken van vitale sectoren lijkt op dit moment dus illusoir. De technische haalbaarheid, juridische armslag, beschikbare kennis en financiële middelen zullen per sector, dienst of product variëren. Het opzetten van een volledige gescheiden ICT-netwerk zal zeer grote investeringen in kennisopbouw en productiecapaciteit vergen, en daarmee erg kostbaar zijn. Om de financiële haalbaarheid van gescheiden netwerken te bepalen is echter een analyse per sector, dienst en product nodig, om gedetailleerd inzicht in de verdeling van kosten en baten te verkrijgen.

Uitspraken ten aanzien van technische haalbaarheid van scheiding van ICT-netwerken kunnen wij bovendien voornamelijk doen op basis van de huidige kennis en stand van zaken, en op basis van onze verwachtingen voor de nabije toekomst. De ontwikkelingen in ICT-infrastructuren neigen naar het steeds verder combineren van netwerken en apparaten. Dit kan tot gevolg hebben dat wat nu een op zichzelf staand netwerk is, dat in de toekomst niet meer is. Daarnaast ontwikkelen de bedreigende actoren en middelen zich ook verder waardoor oplossingen voor nu mogelijk niet houdbaar blijken. Aanleg van (deels) gescheiden netwerken vergt vooruitzien en een lange-termijn planning, maar ook telkens nieuwe analyse van belang, dreiging, weerstand en beschikbare middelen en mogelijkheden. Het kan dan ook zinvol zijn om deze verkenning in de toekomst te herhalen voor de dan geldende bedreigingen, maatregelen en kosten.

De wenselijkheid van een gescheiden netwerk moet beoordeeld worden in relatie tot alternatieve maatregelen op basis van een specifieke risicoanalyse

Het aanleggen van een deels gescheiden ICT-netwerk of cloud is één van de mogelijke remedies die zou kunnen bijdragen aan het verbeteren van de veiligheid van vertrouwelijke (overheids-) data en van vitale diensten.

De wenselijkheid van een gescheiden ICT-netwerk moet beoordeeld worden in vergelijking met alternatieve en/of aanvullende maatregelen, en op basis van een volledige risicoanalyse, zodat kosten en baten van de verschillende alternatieven vergeleken kunnen worden. Er zijn vele andere, deels eenvoudigere en minder kostbare maatregelen denkbaar die een bijdrage kunnen leveren aan het verbeteren van de cybersecurity. Deze maatregelen liggen op het vlak van preventie, detectie en respons. Hierbij kan gedacht worden aan zaken als encryptie, verbeteren van toegangscontrole, training van gebruikers, detectie van incidenten, wetgeving, certificering, accreditatie en audits of het introduceren van ophaalbruggen om netwerkdelen in geval van nood af te koppelen. De twee incidenten die mede de aanleiding hebben gevormd tot dit onderzoek, de DDoS-aanvallen op banken in april 2013 en de onthullingen door Snowden over internationale spionage, illustreren dit. De Nationale Anti DDoS Wasstraat (NAWAS) biedt een mogelijke oplossing voor de bescherming van de beschikbaarheid van diensten, terwijl encryptie bescherming kan bieden voor risico's rond integriteit en vertrouwelijkheid van data.

Gegeven de diversiteit aan vitale diensten, dreigingen en mogelijke mitigerende maatregelen hiertegen, zouden door middel van een risicoanalyse de kans en impact van dreigingen in kaart gebracht kunnen worden, om hier vervolgens mitigerende maatregelen aan te koppelen. In een vervolgstap kunnen dan, afhankelijk van wat men als acceptabele risico's beschouwt, proportionele mitigerende maatregelen worden geïdentificeerd. Dit kan het onder meer het (gedeeltelijk) scheiden van delen van ICT-netwerken omvatten als onderdeel van de maatregelen, maar dat hoeft niet.

Het is bij het adresseren van het wenselijkheidsvraagstuk nodig om uit te gaan van een sector- en dienst-specifieke risicoanalyse. Het is niet goed mogelijk om in *generieke* zin conclusies te trekken ten aanzien van de wenselijkheid van een gescheiden ICT-netwerk. Dit hangt af van een grote hoeveelheid sector- en diensten specifieke factoren en zal altijd een afweging zijn van dreiging, belang en kosten van een gescheiden ICT-netwerk versus alternatieve maatregelen.

Hierbij dient men zich te realiseren dat ook bij volledige scheiding van ICT-netwerken niet alle risico's gemitigeerd zullen zijn: honderd procent veiligheid is onhaalbaar. Uit het *Cybersecuritybeeld Nederland 4* komt naar voren dat staten en cybercriminelen op dit moment de grootste dreiging vormen voor de Nederlandse ICT-infrastructuur. Voornamelijk staten, en in toenemende mate cybercriminelen, hebben aanzienlijke middelen (financieel en technische capaciteiten) om geavanceerde aanvallen uit te voeren op specifieke doelwitten. Ook in het geval van volledige scheiding van ICT-netwerken zal altijd sprake zijn van restrisico's, en dus zal een bepaalde risico-acceptatie onvermijdelijk zijn.

Ook dient de vraag te worden gesteld wat de rol van de overheid zou moeten zijn ten aanzien van gescheiden ICT-netwerken. Zoals vermeld in het *Cybersecuritybeeld Nederland 4* spelen er bij cybersecurity organisatorische, individuele, maatschappelijke en ketenbelangen. Daar waar sprake is van marktfalen in het waarborgen van deze belangen in de vitale sectoren en diensten, is er een rol voor de overheid.

1. Inleiding

1.1. Aanleiding van het maatschappelijk debat rond gescheiden ICT-netwerken

Het maatschappelijk debat over ICT-veiligheid van vitale processen, specifiek over gescheiden ICT-netwerken en -diensten om cybersecurity te waarborgen, is voortgekomen uit een toenemend aantal veiligheidsincidenten. Twee incidenten zijn de directe aanleiding geweest voor het politieke debat rondom gescheiden ICT-netwerken:

- April 2013: grootschalige DDoS (Distributed Denial of Service) aanvallen hebben in Nederland de websites van enkele banken tijdelijk onbereikbaar gemaakt[5]. Tegelijkertijd kregen sommige klanten foutieve saldi te zien, hoewel dit naar verluidt niet gerelateerd was aan de DDoS-aanvallen[6].
- Mei 2013: Edward Snowden lekt documentatie over het bestaan van grootschalige en wereldwijde cyberspionage door de NSA. De lekken zorgen voor debat over de afweging tussen nationale veiligheid en privacy.

Het grote aantal hierop volgende incidenten heeft het debat over de ICT-veiligheid van vitale processen verder aangewakkerd. Voorbeelden hiervan zijn:

- Oktober 2013: De Duitse Bondskanselier is mogelijk afgeluisterd vanuit de Amerikaanse ambassade. De actie zou zijn uitgevoerd door Amerikaanse inlichtingendiensten, die vermoedelijk ook de mobiele telefoon van Merkel afluisterden[7].
- Oktober 2013: Nederlandse hackers hebben bankrekeningen geplunderd en daarbij vermoedelijk een miljoen euro buitgemaakt. Door het sturen van e-mails en tweets met links naar malware konden ze computers van Nederlandse rekeninghouders infecteren, waardoor ze nieuwe betalingsopdrachten konden aanmaken of bestaande opdrachten konden wijzigen.
- Februari 2014: Verschillende Nederlandse internetgebruikers zijn de dupe geworden van telefoniefraude. Door een kwetsbaarheid in de FRITZ!Box-modem die zij gebruikten, werd gebeld naar dure buitenlandse telefoonnummers zonder dat ze dat zelf wisten[9]. Dit kan gezien worden als een voorbeeld van de kwetsbaarheid van apparaten die verbonden zijn met internet. De Economist heeft deze kwetsbaarheid al vervat in de waarschuwing om *the Internet of Things* niet te laten verworden tot *the Internet of Things to be hacked*[8].
- April 2014: De (al jaren aanwezige) Heartbleed-kwetsbaarheid wordt bekend. Hiermee kunnen actoren op afstand het internetgeheugen lezen van systemen die OpenSSL gebruiken[9], zodat bijvoorbeeld gebruikersnamen, wachtwoorden en private keys van beveiligingscertificaten achterhaald kunnen worden.

In algemene zin betreffen cybersecurity incidenten inbreuken met motieven als politieke en economische spionage, geldelijk gewin en verstoring van de beschikbaarheid van vitale infrastructuren[9]. Zo geeft de AIVD aan[10] dat ook Nederlandse bedrijven doelwit zijn geweest van zeer gerichte aanvallen waarbij op grote schaal hoogwaardige technologische informatie en vertrouwelijke bedrijfsinformatie zijn weggesluisd. Deze aanvallen vormen een concrete dreiging voor de omzet, concurrentiepositie, werkgelegenheid en winstgevendheid. Ook de Nederlandse ICT-infrastructuur op zichzelf is hierbij doelwit, en fungeert vaak ongewild als 'doorvoerhaven' van aanvallen.

---

[5] Interbancair en internationaal netwerkverkeer van banken wordt afgehandeld middels (deels) gescheiden netwerken, zodat niet gesteld kan worden dat bij de DDoS-aanvallen op de web-omgevingen van banken, het stelsel van betalingsverkeer zelf onder druk heeft gestaan.

[6] Persbericht ING, 5 april 2013.

[7] *NSA-Überwachung: Merkels Handy steht seit 2002 auf US-Abhörliste,* 26 oktober 2013 zie: http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html.

[8] *Special report on cyber-security*, The Economist, 12 juli 2014.

[9] *Cybersecuritybeeld Nederland-4 CSBN-4*, Nationaal Cyber Security Centrum, juli 2014.

[10] *Jaarverslag*, Algemene Inlichtingen- en Veiligheidsdienst, 2013.

Beveiligingsbedrijf McAfee en het Center for Strategic and International Studies schatten in juni 2014 in dat Cybercrime in Nederland jaarlijks een verlies oplevert van 1,5 procent van het Bruto Binnenlands Product[11], ofwel 8,8 miljard Euro in 2013. Dit percentage ligt relatief hoog ten opzichte van andere landen en leidde tot vragen in de Tweede Kamer[12].

Naarmate het belang en de waarde van ICT in de samenleving toeneemt, wordt de impact van ICT-risico's voor de veiligheid van individuen, bedrijven en overheden groter. Een complexiteit daarbij is dat ICT-netwerken van vitale Nederlandse processen zijn verknoopt met het Internet. Deze verbinding faciliteert de innovaties waar het Internet voor staat maar heeft als keerzijde dat kwaadwillenden van waar ook ter wereld de aanval kunnen openen op Nederlandse ICT-voorzieningen.

1.2. Aanleiding van dit onderzoek

De DDoS-aanvallen op banken in 2013 en de internationale spionageonthullingen van Edward Snowden waren de directe aanleiding voor de Minister van Veiligheid en Justitie om in de *Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam* (NCSS-2)[13] het volgende toe te zeggen:

"Er wordt een verkenning uitgevoerd in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. Met een gescheiden netwerk nemen de mogelijkheden om de continuïteit van vitale processen te borgen toe. Ook kunnen binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld. Hierdoor kan de privacy/integriteit van de data in deze opslag of cloud worden verbeterd".

Deze toezegging volgt mede op de zorg die in de Tweede Kamer is ontstaan over de opslag van vertrouwelijke data. In november 2013 nam de Tweede Kamer een motie van PvdA en VVD aan, die de regering opriep om "privacygevoelige gegevens van onze burgers uitsluitend op servers op te slaan die onder de Nederlandse wetgeving vallen, om weglekken naar buitenlandse partijen of naar commerciële partijen te voorkomen." [14] In mei 2014 vroegen Kamerleden aan de Minister van Binnenlandse Zaken welke stappen hij gaat ondernemen om alle vertrouwelijke data van overheidsorganisaties en semipublieke instellingen binnen Nederland te houden, of anderszins te waarborgen dat buitenlandse veiligheidsdiensten zich geen toegang kunnen verschaffen tot deze vertrouwelijke data[15]. De Minister heeft in antwoord hierop[16] aangegeven dat de Rijksoverheid heeft gekozen om een Rijkscloud in te richten als een voorziening die generieke diensten gebaseerd op cloudtechnologie levert binnen de Rijksdienst. Deze voorziening wordt ingericht op basis van een eigen beveiligd netwerk en in vier Overheidsdatacenters. Strikte eisen hierbij zijn "*dat de gegevens in Nederland blijven, de veiligheid voor alle afnemers adequaat is, en op een voor de gekozen toepassingen acceptabel niveau kan worden geregeld*".

Vergelijkbare zorgen over de veiligheid van ICT en dataopslag zijn echter ook van toepassing op andere Nederlandse vitale producten, diensten en processen. Deze maken gebruik van eigen ICT-voorzieningen die in zowel publiek als privaat eigendom zijn. Terugkerende thema's zijn hierbij zorgen over het commercieel gebruik van vertrouwelijke gegevens en persoonsgegevens door markpartijen, vragen over onder wel juridisch stelsel data valt, waaronder de reikwijdte van de Amerikaanse Patriot Act[17] en de kwetsbaarheid van deze ICT-voorzieningen voor cybercrime.

---

[11] *Net Losses: Estimating the Global Cost of Cybercrime,* McAfee en Center for Strategic and International Studies, juni 2014

[12] *Beantwoording Kamervragen over bericht dat cybercrime Nederland jaarlijks 8,8 miljard euro kost,* De Minister van Veiligheid en Justitie, I.W. Opstelten, augustus 2014.

[13] *De Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam*, Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Veiligheid en Justitie, 2013.

[14] Notitie *Vrijheid en veiligheid in de digitale samenleving*, Kamerstuk 13 december 2013.

[15] Vragen van de leden De Liefde, Moors, Dijkhoff en Litjens aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over de opslag van vertrouwelijke data door overheidsorganisaties en semi-publieke instellingen (ingezonden 27 mei 2014).

[16] Antwoorden op schriftelijke vragen van de leden De Liefde, Moors, Dijkhoff en Litjens aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over de opslag van vertrouwelijke data door overheidsorganisaties en semi-publieke instellingen (ingezonden 4 juli 2014).

[17] Amerikaanse wetgeving die geïntroduceerd is als reactie op de aanslagen van 11 september 2001, met als doel meer mogelijkheden te geven aan de Amerikaanse overheid om informatie te vergaren over en op te treden in geval van mogelijk terrorisme.

1.3. Doelstelling, vraagstelling en reikwijdte van dit onderzoek

PwC heeft op verzoek van de NCTV een verkennend onderzoek uitgevoerd naar in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. In dit rapport zal kortweg gesproken worden over *gescheiden ICT-netwerken*, of *gescheiden netwerken*. Met ICT-netwerken doelt men op het geheel van apparaten die door middel van kabel- of draadloze verbindingen, via routers die het dataverkeer sturen, in verbinding staan met andere apparaten en ICT-diensten, waaronder clouddiensten.

De hoofdvraag in dit rapport is: *zijn gescheiden ICT-netwerken in Nederland* ***haalbaar*** *en* ***wenselijk***?

Het betreft hier nadrukkelijk een eerste verkenning, uitgevoerd in een zeer korte doorlooptijd. Dit rapport bevat dan ook een beknopte, descriptieve verkenning op hoofdlijnen, zonder definitieve aanbevelingen. Wat betreft de reikwijdte geldt bovendien dat ten aanzien van de haalbaarheid van gescheiden ICT-netwerken en diensten weliswaar aandacht wordt besteed aan economische aspecten, maar dat het geen volledige maatschappelijke kosten en batenanalyse betreft.

Het onderzoek en deze rapportage richten zich op de rol van gescheiden ICT-netwerken binnen de rijksoverheid en vitale sectoren van de Nederlandse maatschappij. Dit sluit echter niet noodzakelijkerwijs uit dat er goede lessen te trekken zijn uit voorbeelden van gescheiden ICT-netwerken in andere sectoren.

1.4. Onderzoeksbenadering

Het onderzoek is gebaseerd op een drietal soorten bronnen:

1. individuele interviews met leden van de stuurgroep Gescheiden Netwerken, bestaande uit publieke en private partijen (zie appendix A voor de samenstelling van deze stuurgroep);
2. een drietal discussiesessies met experts en belanghebbenden uit zowel de publieke als private sector waaronder de vitale sectoren, die zijn geselecteerd in overleg met NCTV (zie appendix A voor de organisaties die de deelnemers aan deze sessies vertegenwoordigden); en
3. onderzoek op basis van informatie die beschikbaar is in open bronnen, informatie die is aangereikt door NCTV en de informatie die is verkregen naar aanleiding van de discussiesessies.

De gehanteerde onderzoeksbenadering is daarbij als volgt:

- Allereerst hebben wij uiteen gezet waar men naar streeft met cybersecurity en welke dreigingen men met gescheiden netwerken zou moeten wegnemen.
- Vervolgens hebben we een theoretisch kader geschetst voor de manieren waarop men netwerken kan scheiden, en geven een definitie van volledig gescheiden netwerken.
- Aan de hand van dit kader zijn we op zoek gegaan naar bestaande voorbeelden van gescheiden netwerken in Nederland en in het buitenland.
- Op basis van het theoretisch kader en de voorbeelden worden bevindingen gepresenteerd over de wenselijkheid en haalbaarheid van gescheiden netwerken.

2. *Theorie: een theoretisch kader biedt handvatten voor een gestructureerde discussie*

2.1. Cybersecurity kent drie gerelateerde aspecten: beschikbaarheid, integriteit en vertrouwelijkheid

ICT is overal. Wij bewaren veel van onze gegevens en kennis elektronisch en zijn hiervoor aangewezen op computersystemen en telecommunicatienetwerken. ICT ondersteunt bedrijfsprocessen en bedient allerlei complexe processen in vitale infrastructuren. Bovendien zijn steeds meer ICT-middelen en -diensten met elkaar verbonden. Dit conglomeraat van ICT-middelen en -diensten, dat alle entiteiten die digitaal verbonden kunnen zijn omvat, noemen we het cyberdomein. Het cyberdomein omvat zowel permanente als tijdelijke of plaatselijke verbindingen, evenals de gegevens die zich in dit domein bevinden, waarbij geen geografische beperkingen zijn gesteld[18].

ICT-verbindingen zijn dus een essentieel onderdeel van het cyberdomein. De verbindingen faciliteren het efficiënt opslaan, delen en gebruiken van informatie op geografisch gescheiden locaties. Om de veiligheid van computersystemen en telecommunicatienetwerken te vergroten, is daarbij vaak sprake van een redundante uitvoering. Systemen en/of verbindingen worden dan dubbel uitgevoerd, idealiter op verschillende locaties of langs verschillende routes, zodat bij uitval van een van de systemen of verbindingen, het andere systeem of verbinding kan inspringen. Toch blijven er risico's bestaan. Het toenemende belang van ICT vergroot de impact indien deze risico's zich manifesteren. Naar schatting van het ministerie van Economische Zaken is 60% van onze economische groei tussen 1995 en 2005 gekoppeld aan ICT[19]. Er is dus een toenemende noodzaak om het cyberdomein veilig te houden, met name wanneer het informatie van de Rijksoverheid en vitale processen betreft. Zoals beschreven in de Nationale Cyber Security Strategie 2[20] wordt cybersecurity gedefinieerd als:

Het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. De schade kan bestaan uit: aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.

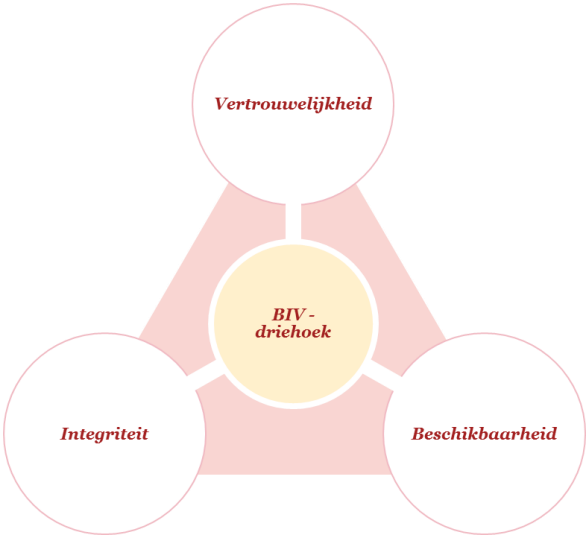
In deze definitie wordt gebruik gemaakt van de Beschikbaarheid, Integriteit, Vertrouwelijkheid (BIV) indeling, een gangbare indeling in cybersecurity, waarmee veiligheid wordt beschreven aan de hand van drie aspecten. Deze aspecten kan men als volgt beschrijven:

- **Beschikbaarheid** heeft betrekking op de mogelijkheid gebruik te maken van de dienst op de afgesproken tijden, waarbij aspecten als *tijdigheid*, *continuïteit* en *robuustheid* een rol spelen.
- **Integriteit** heeft betrekking op de *juistheid* en *volledigheid* van de data.
- **Vertrouwelijkheid** heeft betrekking op de *privacy* van de data, en de *exclusiviteit van de toegang* daartoe.

[18] Voorgaande beschrijving is gebaseerd op de *Nationale Cybersecurity Strategie 2*, NCTV, Ministerie van Veiligheid en Justitie, 2013, de handreiking *Cybercrime, van herkenning tot aangifte*, Nationaal Cyber Security Centrum, 2012.

[19] *ICT en economie,* Ministerie van Economische zaken, http://www.rijksoverheid.nl/onderwerpen/ict/ict-en-economie, 15 augustus 2014.

[20] *De Nationale Cybersecurity Strategie 2*, Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Veiligheid en Justitie, 2013.



Figuur 1. BIV-driehoek indeling van aspecten van veiligheid in het cyberdomein.

Afhankelijk van de toepassing van het ICT-netwerk of de ICT-dienst zal een specifieke balans gezocht worden tussen deze drie aspecten. Zo zal voor ICT-voorzieningen die cruciaal zijn voor de levering van elektriciteit, gas of water, de permanente beschikbaarheid van het grootste belang zijn. In de gezondheidszorg zijn beschikbaarheid, integriteit en vertrouwelijkheid van patiëntgegevens alle drie van groot belang. Bij financiële transacties zal de nadruk liggen op vertrouwelijkheid en integriteit van financiële gegevens en de beschikbaarheid van de het betalingsverkeer. Voor overheidsinformatie over bijvoorbeeld persoonsgegevens van burgers zal vertrouwelijkheid en integriteit van groot belang zijn.

Er is vaak ook sprake van een afwegingsrelatie tussen de genoemde BIV-aspecten. Zo kan encryptie, ofwel versleuteling van informatie, de vertrouwelijkheid verbeteren maar tegelijk beschikbaarheidsaspecten verminderen. Encryptie vereist extra capaciteit van ICT-infrastructuren en vraagt mogelijk om extra handelingen van gebruikers. Redundantie, ofwel het dubbel uitvoeren, van netwerkverbindingen kan de beschikbaarheid ervan verbeteren, doordat er een extra lijn is om op terug te vallen. Dit kan tegelijk juist weer een extra kwetsbaar punt introduceren waarop een kwaadwillende kan inbreken en bijvoorbeeld de vertrouwelijkheid kan schaden.

Doordat voor verschillende toepassingen een andere optimale balans tussen de drie veiligheidsaspecten zal gelden, zullen maatregelen ten behoeve van het verbeteren van cybersecurity dan ook verschillen, afhankelijk van het belang van de toepassing, de bedreigingen, de weerstand en de resulterende risico's. Ten aanzien van een gescheiden ICT-netwerk voor vitale processen kan daarom de vraag gesteld worden welke BIV-drijfveer geldt: is het *one size fits all*? De afweging zal niet in een isolement plaatsvinden, maar in een context waar onder andere beschikbare techniek, beschikbare kennis en geld een belangrijke rol spelen.

2.2. Cyberdreigingen komen uit verschillende hoeken, op basis van verschillende motiveringen

De huidige discussie over cybersecurity van vitale sectoren en diensten draait rond verweer tegen bedreigende actoren die DDoS-aanvallen plegen en spioneren. Het handelen van deze actoren zorgt voor risico's voor de belangen van individuen, organisaties, ketens en de maatschappij als geheel ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid van data en systemen.

Deze belangen materialiseren zich in zaken als consumentendata, informatie over financiële markten en zakelijke overeenkomsten, informatie over geavanceerde productietechnieken, research & development gegevens, gezondheidsgegevens, de proces controle systemen[21] waarmee vitale infrastructuur op afstand wordt aangestuurd, en militaire informatie.

[21] (SCADA, Supervisory Control And Data Acquisition).

Kwaadwillenden zijn, afhankelijk van hun aard, intenties en vaardigheden, uit op verschillende van dergelijke doelwitten. Het Cybersecuritybeeld Nederland-4 (CSBN-4) van het NCSC geeft een overzicht van deze dreigers en hun doelwitten (Tabel 1).

Tabel 1. Overzicht dreigingsniveau (bron: Cybersecuritybeeld Nederland-4, NCSC).

Actoren (Dreigers)	Overheden	Private organisaties	Burgers
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Cyberaanvallen	Cyberaanvallen	
Terroristen	Verstoring/overname ICT	Verstoring/overname ICT	
(Beroeps-) criminelen	Diefstal en publicatie of verkoop van informatie ↓	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie ↑
	Manipulatie van informatie ↓	Manipulatie van informatie ↓	Manipulatie van informatie
	Verstoring ICT ↑	Verstoring ICT ↑	Verstoring ICT ★
	Overname ICT ↓	Overname ICT ↑	Overname ICT
Cybervandalen en scriptkiddies	Diefstal informatie ↓	Diefstal informatie ↓	Diefstal informatie
	Verstoring ICT ↓	Verstoring ICT	
Hacktivisten	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie
	Bekladding van ICT	Bekladding van ICT	
	Verstoring van ICT	Verstoring ICT	
	Overname ICT ★	Overname ICT	
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie	
	Verstoring ICT	Verstoring ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private organisaties		Diefstal van informatie (bedrijfsspionage) ↓	
Geen actor	Uitval ICT	Uitval ICT	Uitval ICT

Legenda relevantie

Laag	Midden	Hoog
Er worden geen nieuwe trends of fenomenen waargenomen waarvan dreiging uitgaat. OF Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. OF Er hebben zich geen noemenswaardige incidenten voorgedaan in de rapportageperiode.	Er worden nieuwe trends en fenomenen waargenomen waarvan dreiging uitgaat. OF Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen. OF Incidenten hebben zich (op enkele kleine na) vooral voorgedaan buiten Nederland.	Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken. OF Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. OF Incidenten hebben zich voorgedaan in Nederland.

↑ Dreiging is toegenomen ↓ Dreiging is afgenomen ★ Dreiging is nieuw

Uit het CSBN-4 komt naar voren dat staten en cybercriminelen op dit moment de grootste dreiging vormen voor Nederlandse ICT-infrastructuur. Staten zijn gericht op digitale spionage en offensieve capaciteiten en investeren actief in hun capaciteiten om cyberoorlog te voeren. Criminelen hebben een sterkere focus op diefstal en manipulatie van informatie voor geldelijk gewin. Er ontwikkelt zich een professionele dienstensector voor cybercriminaliteit, waarbij de middelen om cyberaanvallen uit te voeren steeds meer gemeengoed worden. Dit zal uiteindelijk de cybercrimevaardigheden van cybervandalen, hacktivisten en interne actoren op een hoger niveau brengen. De gereedschapskist van deze actoren loopt zeer uiteen.

Zo kunnen zij door middel van *social engineering* toegang tot ICT verkrijgen maar ook actief inbreken via geavanceerde digitale gereedschappen. Een gescheiden netwerk moet zich dus tegen vele mogelijke combinaties van bedreigende actoren en hulpmiddelen wapenen.

2.3. Wat is een gescheiden ICT-netwerk?

Scheiding van ICT-netwerken wordt in het maatschappelijke en politieke debat opgeworpen als een mogelijke remedie tegen cybersecurity dreigingen. Daarbij bestaan verschillende visies op de doelstelling van het scheiden van netwerken en zijn er verschillende interpretaties over wat het scheiden van netwerken precies impliceert.

In de *Nationale Cyber Security Strategie 2* wordt gesproken over een gescheiden ICT-netwerk voor publieke en private vitale processen. In deze paragraaf zullen we allereerst ingaan op wat een ICT-netwerk is. Vervolgens gaan we in op mogelijke niveaus van scheiding van een ICT netwerk. We verduidelijken dit door drie verschillende perspectieven op het scheiden van een ICT-netwerk te hanteren: de productieketen, de netwerkhiërarchie niveaus, en fysieke versus virtuele scheiding.

2.3.1. Een ICT-netwerk

ICT-netwerken lopen uiteen van wereldwijd aaneengeschakelde netwerken tot plaatselijke netwerken van organisaties, huishoudens of individuen. In algemene zin bestaan ICT-netwerken uit computers/servers, die via kabel- of draadloze verbindingen, en routers die het dataverkeer routeren, in verbinding staan met andere computers/servers. Steeds vaker zijn plaatselijke netwerken via het Internet gekoppeld aan andere plaatselijke netwerken. In een sterk vereenvoudigd beeld zijn Nederlandse afnemers en aanbieders van ICT-diensten op de volgende manier met het internet verbonden, van globaal naar lokaal:

- Onderzeese glasvezelkabels verbinden verschillende continenten met elkaar via belangrijke internationale knooppunten. Eén van deze knooppunten is de Amsterdam Internet Exchange.
- Deze knooppunten of Internet Exchanges zijn onderling met elkaar verbonden en vormen op hun beurt een wereldwijd spinnenweb waarover internetverkeer kan lopen.
- Internetproviders krijgen toegang tot het wereldwijde netwerk door zich met een verbinding aan te sluiten op één van deze Internet Exchanges. Zo zijn Nederlandse internetproviders als KPN, Ziggo en UPC onder andere aangesloten op de Amsterdam Internet Exchange of leggen direct koppeling met buitenlandse exchanges zoals de DE-CIX in Frankfurt. Veel internetproviders zijn bovendien direct met elkaar gekoppeld voor het afhandelen van dataverkeer.
- Gebruikers van ICT-diensten sluiten zich aan op een internetprovider via lokale fysieke of draadloze verbindingen zoals DSL, coax, glasvezel, Wi-Fi en 4G. Deze hebben verschillende niveaus van beveiliging, robuustheid en capaciteit. Exclusieve huur- of leaselijnen zijn beschikbaar voor organisaties die hogere eisen aan de beschikbaarheid, capaciteit en vertrouwelijkheid van hun verbinding.
- Aanbieders van ICT-diensten met hoge eisen aan beschikbaarheid, waaronder clouddiensten, kunnen een eigen backbone verbinding afnemen naar één of meerdere Internet Exchange punten. Dergelijke verbindingen zijn vergelijkbaar met die van de internetproviders naar de Internet Exchanges.
- Op lokaal niveau vormen zich binnen organisaties ook weer netwerken van netwerken. Zo koppelen rijksoverheden, deel- en semioverheden hun netwerken en zullen bedrijven de ICT-netwerken van hun leveranciers en afnemers aan elkaar koppelen.
- Binnen organisaties en huishoudens wordt de verbinding met het wereldwijde internet door routers gesplitst over meerdere apparaten en gebruikers. Deze routers zijn weer via bijvoorbeeld ethernetkabels of draadloze verbindingen zoals Wi-Fi of femtocellen verbonden met computers.

Het systeem van meerdere knooppunten houdt in dat internetverkeer meerdere routes kan nemen om op de plaats van bestemming te komen, ook als delen van het internet niet beschikbaar zijn of met capaciteitsproblemen te kampen hebben. Daarbij is het bovendien zo dat gegevensbestanden opgeknipt in delen over het internet worden verstuurd, waarbij individuele delen van een gegevensbestand over verschillende routes kunnen worden vervoerd. Op de plaats van bestemming aangekomen worden ze dan weer samengevoegd.

Dit heeft zijn oorsprong in de initiële doelstellingen van het internet, namelijk het bieden van een netwerk dat in staat zou zijn om grootschalige uitval van onbetrouwbare knooppunten en verbindingen op te vangen.

Het internet zelf kan men omschrijven als een netwerk van netwerken. Het is aan veel - maar niet alle - lokale netwerken gekoppeld, en stelt het dataverkeer in staat meerdere routes te nemen. Vaak is bovendien zo dat ook de infrastructuren van de vitale sectoren via internet verbonden zijn met andere punten in de wereld. Dit is de laatste jaren steeds gangbaarder geworden, omdat het voor veel bedrijven een manier is om innovatiever en tegen lagere kosten te opereren, bijvoorbeeld door op afstand infrastructuur voor onderhoudsdoeleinden te laten monitoren.

Niet alle netwerken zijn aan het internet gekoppeld. Organisaties kunnen bijvoorbeeld lokale netwerken opzetten waarop de informatie van hun kantoorautomatisering wordt uitgewisseld. Deze netwerken zijn in de praktijk dikwijls gescheiden van het Internet door middel van een *Demilitarized Zone* ofwel DMZ. Individuen kunnen ook thuisnetwerken opzetten van laptops, personal computers en printers die zonder internetverbinding opereren. Hoewel dergelijke netwerken niet aan het Internet zijn gekoppeld maken ze alsnog gebruik van de onderliggende netwerktechnologie die ten grondslag ligt aan het Internet om data rond te sturen binnen hun besloten netwerk. Dit betekent dat ze vergelijkbare kwetsbaarheden bevatten die misbruikt kunnen worden voor verstoring, diefstal, overname en bekladding van ICT indien kwaadwillenden zich toegang tot (onderdelen van) dergelijke lokale netwerken weten te verschaffen. Hoewel het Internet dan niet meer als toegangsroute voor bedreigende actoren fungeert, is hun gereedschapskist nog steeds bruikbaar. Zo zijn huurlijnen die kantoorgebouwen onderling verbinden gevoelig voor vergelijkbare inbraakmiddelen als huurlijnen die een kantoorgebouw verbinden met het Internet.

Nederlandse ICT-netwerken zijn dus op veel verschillende punten verbonden met andere ICT-netwerken, waaronder ICT-netwerken in andere landen. De volgende secties belichten een drietal perspectieven op het scheiden van ICT-netwerken, ten behoeve van een discussie over de haalbaarheid en wenselijkheid van gescheiden ICT-netwerken.

2.3.2. *De productieketen*

Allereerst nemen wij de productieketen van een ICT-netwerk in ogenschouw (Figuur 2). Onderstaande keten onderscheidt zes stappen en geeft voorbeelden van mogelijke risico's in elke stap. De overweging hierbij is dat de bouw, de exploitatie en het onderhoud van een eventueel gescheiden ICT-netwerk in de context van een internationale productieketen plaatsvindt. De scheiding van het ICT-netwerk op zich is dan niet voldoende om de veiligheid van dat netwerk te garanderen. Een deel van de kwetsbaarheid van netwerken vindt immers zijn oorsprong in de keten van ontwerp en bouw van netwerkcomponenten tot upgrades van het netwerk: welke kwetsbaarheden zijn, al dan niet bewust, in componenten ingebouwd?

Figuur 2. De stappen in de productieketen van een ICT-netwerk, inclusief voorbeelden van risico's in elke stap.

In de huidige situatie bestaat een wederzijdse afhankelijkheid van leveranciers van ICT-producten en diensten uit verschillende landen. Deze leveranciers voldoen aan uiteenlopende eisen die voorvloeien uit onder meer nationale wet- en regelgeving. Organisaties die ICT-producten en -diensten aanschaffen zijn zich niet altijd bewust van waar de individuele hardware en software componenten van afkomstig zijn en hoe deze geproduceerd zijn. Dit kan risico's opleveren voor de organisatie die de producten aanschaft. Dreigingen in de keten kunnen echter ook buiten de leverancier van netwerkapparatuur ontstaan, bijvoorbeeld:

- Tijdens het productieproces van netwerkcomponenten kunnen kwaadwillenden software aanpassen.
- Bij transport kunnen onderdelen vervangen worden door onderdelen met kwetsbaarheden.
- De bouw van het netwerk biedt gelegenheid om aftapapparatuur te plaatsen.
- Het proces van beheer en gebruik van het netwerk brengt risico's met zich mee op onderhoudsmomenten, via kwetsbaarheden in software upgrades of door onzorgvuldig gebruik.

Het meest bekende voorbeeld van dreigingen in het ontwerp is terug te zien in de discussie in 2012 en 2013 over een aantal Chinese telecomconcerns, wier apparatuur naar verluidt achterdeuren voor spionagedoeleinden zou bevatten[22]. In 2002 vond er een soortgelijke discussie plaats in Nederland over een mogelijke achterdeur in de aftapsoftware van de AIVD, die geleverd werd door een Israëlisch bedrijf[23].

De consequentie is dat zelfs het aanleggen van een fysiek gescheiden netwerk, bijvoorbeeld in de vorm van eigen geulen met eigen glasvezelkabels, geen veiligheid waarborgt als er elders in de productieketen alsnog sprake is van afhankelijkheid van externe leveranciers. Een eerste stap richting meer vergaande scheiding is dat het netwerkonderhoud en -beheer binnenshuis wordt uitgevoerd. In de meeste extreme, meest veilige vorm zou een gescheiden ICT-netwerk echter vanaf de individuele componenten ontworpen en gebouwd moeten worden door de Nederlandse overheid zelf. Dit vergt een afweging tussen veiligheid en de inzet van middelen: zowel de financiële als de praktische haalbaarheid van ketenscheiding neemt af naarmate er tot dieper in de productieketen veiligheid gegarandeerd dient te worden, omdat dit significante investeringen in zowel kennis als productiecapaciteit vereist. Hierbij spelen overwegingen van technische, juridische en financiële aard een rol. De laatste stand van de techniek op het gebied van ICT vraagt vaak betrokkenheid van buitenlandse bedrijven. Bovendien dienen Nederlandse overheden bij inkoop van ICT naast de nationale veiligheid het geldende aanbestedingsrecht in aanmerking te nemen. Ten slotte nemen de kosten van een netwerk toe bij 'insourcing' van de productieketen.

Als alternatief voor insourcing van de volledige keten geldt dat men gebruik kan maken van commerciële bedrijven waarvan de betrouwbaarheid gewaarborgd kan worden, dat gebruik wordt gemaakt van gecertificeerde producten, of een combinatie van beide. De NATO heeft bijvoorbeeld strikte richtlijnen voor cryptografische producten, waarbij bovendien als eis geldt dat deze alleen in een NATO lidstaat mogen zijn geproduceerd[24]. Doordat er minder aanbieders en gecertificeerde producten zijn, maar wel vraag, kan dit echter leiden tot een hoger prijsniveau.

Bij het scheiden van netwerken dient men dus rekening te houden met het bestaan van ketenrisico's. Dat is echter niet voldoende. Dit wordt toegelicht in de volgende twee paragrafen, die ingaan op scheiding van netwerken op verschillende niveaus in de netwerkhiërarchie en op fysieke versus virtuele scheiding van netwerken.

[22] *U.S. Panel Cites Risks in Chinese Equipment*, New York Times, 8 oktober 2012.
[23] *De afluisteraars van de afluisteraars*, Vrij Nederland, 16 juli 2013.
[24] *Cryptograhpic products and Cryptographic Mechanisms*, 11 augustus 2014, http://www.ia.nato.int/niapc/Information/NIAPC-vendor-info.

2.3.3. De netwerkhiërarchie niveaus

Naast de mate van scheiding door de productieketen, kan gekeken worden naar de mate waarin de scheiding wordt doorgetrokken door de verschillende hiërarchische niveaus van ICT-netwerken (Figuur 3). Hierbij wordt het onderscheid gemaakt op basis van de fysieke structuur van een telecomnetwerk, waarbij de communicatie verloopt van of naar:

- centrale dienstplatformen of servers van bijvoorbeeld cloud computing leveranciers;
- een kernnetwerk bestaande uit routers en hoofdverbindingen;
- de toegangslijnen van/naar de individuele huizen of kantoren, inclusief een eventueel binnennetwerk;
- de terminals in de vorm van PCs, laptops, tablets, smartphones en andere apparatuur;
- de uiteindelijke gebruiker.

Figuur 3. De netwerkhiërarchie niveaus

Op elk van deze niveaus kan sprake zijn van gescheiden netwerken of gescheiden toegang tot deze netwerken. Dit kan de vorm aannemen van fysieke scheiding of scheiding op andere wijze, hetgeen wat verschillen in restrisico's met zich meebrengt. Fysieke versus niet-fysieke scheidingsvormen worden nader toegelicht in paragraaf 2.3.4. Voorbeelden van overblijvende restrisico's worden gegeven in paragraaf 4.1.

In de praktijk zijn gedeeltelijke scheidingsvormen bij veel organisaties gemeengoed. Zo houdt **gebruikersscheiding** in dat een selecte groep gebruikers geautoriseerd wordt om toegang te krijgen tot de ICT-voorzieningen van een organisatie. In aanvulling hierop is vaak sprake van **terminalscheiding:** alleen geautoriseerde computers en mobiele apparaten krijgen toegang tot ICT-voorzieningen. Daarnaast kunnen organisaties gebruik maken van **toegangsnetwerkscheiding** bijvoorbeeld door een eigen draadloos netwerk aan te leggen.

Zowel bij scheiding in de productieketen als in de ICT-netwerkketen dient dus tevens een compromis gezocht te worden tussen de wenselijkheid van netwerkscheiding en de haalbaarheid ervan. Paragraaf 3.2 illustreert aan de hand van bestaande voorbeelden van gescheiden netwerken nader hoe hierin keuzes zijn gemaakt.

Een geografisch perspectief op netwerkscheiding: illustratie aan de hand van cloud computing

Een aanvullend perspectief op netwerkscheiding is *geografische scheiding*, wat impliceert dat bepaalde vitale processen en data geografische grenzen, zoals de landsgrenzen, niet mogen of zelfs kunnen verlaten. Dit kan nodig zijn om het toepasbaar zijn van bepaalde buitenlandse wetgeving te vermijden (*juridische scheiding)*. Geografische scheiding kan bovendien wenselijk zijn om toezicht te houden op waar data zich bevindt en wie er fysiek toegang toe heeft. In een antwoord op Kamervragen over cloud dataopslag geeft de minister van Binnenlandse Zaken en Koninkrijksrelaties aan dat het op dit moment niet mogelijk is om aan te wijzen op welke datacenters en in welke landen data van de Nederlandse overheid zich bevindt[1]. We illustreren deze vorm van scheiding aan de hand van cloud computing, dat we als volgt definiëren:

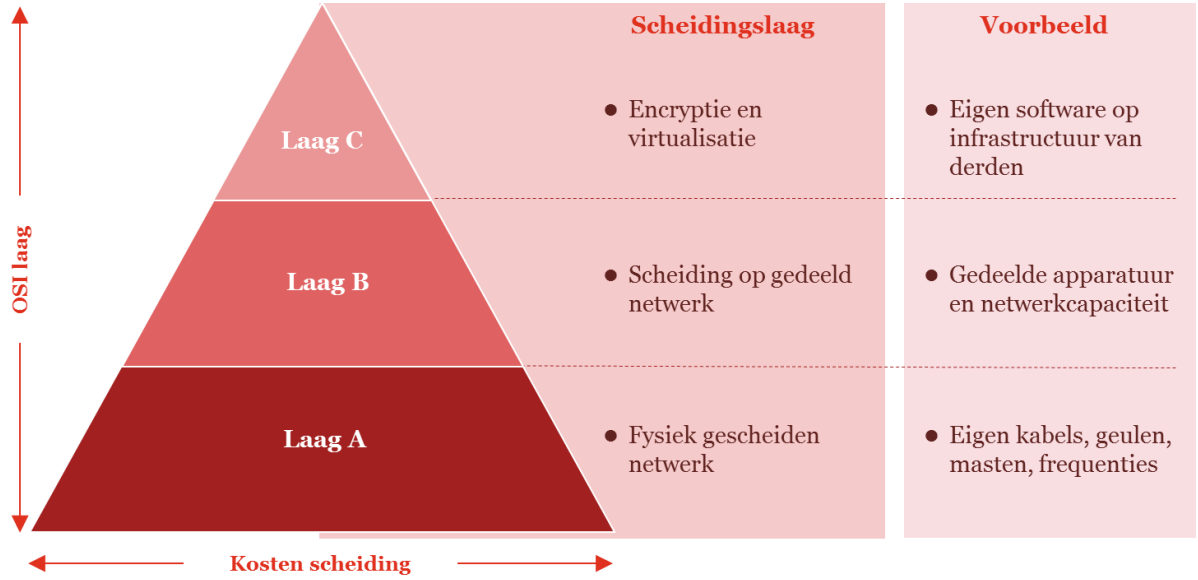
Cloud computing omvat het op afstand gebruik maken van omvangrijke computerbronnen in datacenters met een groot aantal gekoppelde servers met daarin computerbronnen zoals rekenkracht, geheugencapaciteit en specifieke diensten. Deze datacenters kunnen geografisch verspreid zijn terwijl de eindgebruiker ze als één geheel waarneemt. Een individueel databestand opgeslagen in een clouddienst kan zich daardoor in stukken verdeeld op meerdere geografische locaties bevinden. Een ander kenmerkend aspect van cloud computing is dat capaciteit gedeeld wordt over grote groepen gebruikers, om schaalvoordelen te bereiken in de bezettingsgraad van het datacenter en daarmee kosten te reduceren voor de leveranciers en afnemers van clouddiensten. Gebruikers merken geografische scheiding en het delen van clouddiensten zelf niet door virtualisatie, een technologie die het voor eindgebruikers doet voorkomen alsof zij hun eigen 'stuk' cloud bezitten.

Geografische scheiding is niet vanzelfsprekend. Een typisch (maar niet noodzakelijk) kenmerk van cloud computing is immers dat de computer bronnen via internet beschikbaar worden gesteld. Zoals in paragraaf 2.3.1 geschetst, is de werking van het internet dusdanig dat informatie via verschillende routes over de wereld op de plaats van bestemming komt. Ook informatie die vanuit Nederland naar een andere Nederlandse locatie wordt verstuurd kan een buitenlandse route nemen. Een verzameling data opgeslagen in de cloud kan verspreid zijn over datacenters in meerdere landen. In veel bestaande cloud computing oplossingen is het technisch niet altijd meer mogelijk om aan te wijzen waar data zich fysiek bevindt. Als gevolg hiervan kunnen hierop meerdere nationale en internationale wetten van toepassing zijn. Zelfs als de data geografisch gescheiden opgeslagen zou kunnen worden, bijvoorbeeld in Nederland, dan zou dit bovendien zo ingericht moeten worden dat toegang tot deze data vanuit het buitenland onmogelijk is gemaakt, ook voor Nederlanders.

Het is wel mogelijk om Nederlandse data te hosten in één of meerdere clouddatacenters op Nederlands grondgebied. Dit betekent echter niet dat deze data ook juridisch gescheiden is van buitenlandse jurisdictie. Hiervoor zou moeten worden gewaarborgd dat data Nederlands grondgebied niet verlaat (bijvoorbeeld door de cloud servers toegankelijk te maken via een volledig gescheiden ICT-netwerk), en bovendien moet rekening gehouden worden met de eventuele extraterritoriale werking van wetgeving waar bedrijven onder kunnen vallen. Voor bepaalde dienstverlening is het echter wenselijk dat data ook in het buitenland beschikbaar is. Voorbeelden hiervan zijn de internationale diplomatieke communicatie en het verstrekken van aangiftegegevens voor in het buitenland woonachtige belastingplichtigen.

2.3.4. *Van virtueel gescheiden tot fysiek gescheiden netwerken*

Een derde perspectief op een ICT-netwerk volgt uit een door de International Organization for Standardization (ISO) gestandaardiseerd referentiemodel voor datacommunicatie, het Open Systems Interconnect (OSI) model. Het volledige OSI-model onderscheidt zeven lagen, waarbij de onderste laag de fysieke infrastructuur representeert. Op dit niveau is er sprake van een fysiek signaal over een signaaldrager, zoals elektrische of optische signalen over koper, glas, of door de lucht. De hogere lagen voegen elk functionaliteit toe, die het mogelijk maken dat fysieke signalen uiteindelijk de vorm krijgen van voor eindgebruikers begrijpelijke informatie zoals tekst en getallen, wat dan het virtuele is in het geheel. In dit rapport hanteren we een vereenvoudigd perspectief op het OSI-model dat bestaat uit drie lagen: de **fysieke laag**, de **capaciteitslaag** en de **virtuele laag** (zie figuur 4)[25]. Deze drie scheidingslagen kan men toepassen op de verschillende niveaus in de netwerkhiërarchie die zijn beschreven in paragraaf 0. Het volledige OSI-model en de relatie daarvan met het hier getoonde vereenvoudigde model is opgenomen in Appendix C.



Figuur 4. Vereenvoudigd en aangepast OSI-model dat de lagen van netwerkscheiding aangeeft.

Netwerkscheiding kan plaatsvinden op verschillende lagen in dit aangepaste OSI-model:

- **Laag A - fysiek:** de meest verregaande en kapitaalintensieve, kostbare vorm van scheiding zou inhouden dat sprake is van aparte, eigen kabels in geval van een vast netwerk, of eigen antennes en gebruik van ongedeelde frequenties in geval van een draadloos netwerk. Dit is bijvoorbeeld het geval bij het C2000-toegangsnetwerk. Dat betreft een netwerk van antennes, die gebruik maken van frequenties die speciaal voor het C2000-netwerk beschikbaar zijn gesteld[26]. Het kan ook inhouden dat men gebruik maakt van eigen servers en datacenters voor cloud computing diensten. Fysieke scheiding kan verschillende drijfveren hebben, waaronder het garanderen van de beschikbare capaciteit of het bemoeilijken van toegang tot een netwerk om risico's voor integriteit en vertrouwelijkheid te verminderen.
- **Laag B - capaciteit:** een scheiding op laag B kan inhouden dat er gebruik wordt gemaakt van gedeelde kabels en antennes, waarbij een vaststaand deel van de capaciteit kabels of antennes wordt gereserveerd. Dit kan gepaard gaan met eigen of gedeelde apparatuur op de knooppunten van verbindingen. Deze vorm van scheiding is onder andere herkenbaar bij virtuele telecomoperators, die geen eigen netwerk hebben maar capaciteit huren op het netwerk van

[25] Voor een gedetailleerde analyse van cybersecurity dreigingen, risico's en maatregelen op de verschillende niveaus in het OSI-model is het zinvol om uit te gaan van het volledige OSI-model. We verwachten echter dat dit niet bijdraagt aan het algemene begrip dat hier beoogd wordt.

[26] Dit wil overigens niet zeggen dat dit netwerk niet voor storingen gevoelig is. Juist een mobiel of draadloos netwerk zal altijd in bepaalde mate kwetsbaar zijn voor krachtige, storende transmissies in dezelfde frequentieband.

providers die een mobiel- koper- of glasvezelnetwerk hebben uitgerold. Dit kan ook tot uiting komen in de vorm van huurlijnen waarbij men de capaciteit voor verbindingen tussen twee punten garandeert. Bij cloud computing diensten delen grote groepen gebruikers eveneens de processorkracht, geheugencapaciteit en opslagcapaciteit van servers in datacenters. Op laag B zijn beschikbaarheid van capaciteit en efficiëntie in kosten en middelen voorname drijfveren.

- **Laag C - virtueel:** tot slot kan er volledig gebruik worden gemaakt van bestaande ICT-infrastructuren van derde partijen, aangevuld met versleuteling en virtualisatie om de vertrouwelijkheid van de communicatie te waarborgen. Een herkenbaar voorbeeld hiervan zijn de Virtual Private Network (VPN) verbindingen die veel organisaties gebruiken om hun medewerkers in staat te stellen van huis uit toegang te verkrijgen tot de interne ICT-netwerken van de organisatie. Dergelijke verbindingen leggen een virtuele 'tunnel' waardoor informatie versleuteld wordt verstuurd zodat deze minder gevoelig is voor onderschepping en inzage. Er is in dit geval geen sprake van gereserveerde capaciteit, maar er wordt gebruik gemaakt van een al beschikbare communicatiedienst.

De hiervoor beschreven drie perspectieven op een gescheiden ICT-netwerk tonen dat scheiding van netwerken langs een glijdende schaal verloopt. De term *gescheiden ICT-netwerk* zal dan ook door verschillende betrokkenen verschillend geduid worden. Wij introduceren daarom het begrip *volledig gescheiden ICT-netwerk* voor een ICT-netwerk dat langs alle genoemde perspectieven (OSI, hiërarchie en productieketen) tot op elke niveau gescheiden is.

3. ***Verkenning:*** *er zijn verschillende voorbeelden van gescheiden ICT-netwerken en gerelateerde ontwikkelingen*

Ook buiten Nederland hebben cybersecurity incidenten en de Snowden-onthullingen tot discussie geleid over gescheiden netwerken en andere noodzakelijk maatregelen om cybersecurity te versterken. Tegelijk zijn er in Nederland al ICT-netwerken die in meer of mindere mate zijn gescheiden, en die als cases kunnen dienen om te onderzoeken of en hoe dit bruikbare cybersecuritymaatregelen zijn. In dit hoofdstuk beschrijven we voorbeelden van ontwikkelingen rond gescheiden netwerken en clouddiensten in het buitenland, evenals al bestaande voorbeelden van gescheiden ICT-netwerken in Nederland.

3.1. Buitenlandse voorbeelden en ontwikkelingen

De discussie over de veiligheid van ICT-netwerken is in meerdere landen in een stroomversnelling geraakt naar aanleiding van incidenten als hacks van SCADA-systemen binnen vitale sectoren, de onthullingen door Snowden en aanvallen van cybercriminelen (zie paragraaf 1.1). Daarbij nemen landen uiteenlopende standpunten in ten aanzien van te nemen maatregelen om cyberdreigingen te mitigeren. Zo komen verschillende perspectieven op scheidingsvormen aan het licht. Jack Moss, de voormalig Chief Security Officer van ICANN (de overkoepelende organisatie met betrekking tot domeinnamen), suggereerde bijvoorbeeld dat vitale sectoren gebruik zouden kunnen maken van zeer strikt beveiligde diensten gelinkt aan Top Level Domeinnamen zoals .secure, in plaats van .com. Ook Shawn Henry, voormalig Assistant Directeur Cyber bij de FBI, sprak in 2011 over een zoektocht naar "alternatieve vormen van communicatie" die oneigenlijke toegang en gebruik tot vitale infrastructuren zouden beperken[27]. Deze sectie beschrijft ter illustratie van de breedte van dit debat enkele voorbeelden, lopende ontwikkelingen en discussies over gescheiden netwerken in verschillende landen.

In deze sectie beschouwen wij:

- landen die zijn getroffen door internationale spionage en hiertoe gescheiden netwerken als mogelijke maatregel aandragen: bijvoorbeeld Duitsland en Brazilië;
- landen die actuele vraagstukken rond dataopslag in de cloud hebben geadresseerd: bijvoorbeeld Noorwegen en Zweden;
- een land met een initiatief vergelijkbaar met de Rijkscloud: bijvoorbeeld Canada;
- een land met een pakket aan cybersecuritymaatregelen: bijvoorbeeld Verenigd Koninkrijk.

De voorbeelden zijn illustratief en niet uitputtend. Voor een uitgebreidere beschrijving van cloudstrategieën en ander beleidskaders bij Nederlandse en buitenlandse overheden rond cloud verwijzen wij naar de notitie Inventarisatie Cloudstrategieën overheden van het ministerie van Binnenlandse Zaken uit 2013[28].

[27] Critical infrastructure networks chart new path to cyber security, Government Security news, http://www.gsnmagazine.com/article/25257/critical_infrastructure_networks_chart_new_path_cy?page=0,1, 16 december 2011.
[28] Notitie Inventarisatie Cloudstrategieën overheden, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 6 augustus 2013.

3.1.1. *Duitsland verkent de mogelijkheden voor een nationaal of Europees internet*

In oktober 2013 kwam het nieuws naar buiten dat Bondskanselier Merkel van Duitsland mogelijk is afgeluisterd vanuit de Amerikaanse ambassade. De spionage zou zijn uitgevoerd door inlichtingendiensten van de Verenigde Staten, die vermoedelijk ook de mobiele telefoon van de Bondskanselier zouden afluisteren. Het nieuws was aanleiding voor een Europese discussie, waarbij de Bondskanselier in februari 2014 aangaf te willen overleggen over de aanleg van een Europees Communicatienetwerk, waarbij e-mail en ander dataverkeer niet door de Verenigde Staten gaan. De Bondskanselier gaf aan het af te keuren dat internetbedrijven hun activiteiten uitvoeren vanuit landen met lage niveaus van gegevensbeveiliging, terwijl ze actief zijn in landen als Duitsland waar gegevensbeveiliging hoog in het vaandel staan[29].

De onthullingen over spionageactiviteiten hebben geleid tot een plan voor de opzet van een Duits internet. In het scenario dat bedrijfsleven en politiek schetsen zou data Duitsland niet moeten verlaten om te voorkomen dat deze vatbaar is voor spionage of onderschepping door buitenlandse mogendheden.

Op dit moment maken sommige Duitse internetproviders gebruik van Amerikaanse dienstverleners zoals Level3 voor het transporteren van data. Dit zou wegens de implicaties van de Patriot Act kunnen betekenen dat zelfs wanneer dataverkeer Duitse bodem nooit verlaat, buitenlandse inlichtingendiensten alsnog toegang hebben tot de data. Telecomprovider Deutsche Telekom heeft aangegeven dat het in samenwerking met andere Duitse internetproviders een netwerk zou kunnen opleveren dat tegen buitenlandse spionageactiviteiten beveiligd is. In het voorstel van Deutsche Telekom zal dataverkeer alleen via Duitse paden lopen indien zowel zender als ontvanger zich in Duitsland bevinden. Technici van het bedrijf geven aan dat ze een dergelijk netwerk voor de gehele Schengen zone kunnen opzetten, waardoor alle landen in dit gebied veilig data onder elkaar kunnen uitwisselen. Deutsche Telekom wijst erop dat er wetgeving nodig is om het project uit te laten voeren om beschuldigingen van competitievervalsing of beperkingen van het dataverkeer te ontlopen[30].

Critici wijzen erop dat het plan van Deutsche Telekom zinloos wordt op het moment dat een klant gebruik maakt van buitenlandse diensten zoals die van Google, waarbij data wordt overgedragen naar buitenlandse infrastructuur en de wetten van het lokale land gelden. Bovendien zou het indruisen tegen de structuur van het internet, waarin data de snelste en optimale weg naar zijn bestemming moet kunnen vinden. Daarnaast wijst men erop dat hoewel een nationaal netwerk spionage door buitenlandse mogendheden wellicht voorkomt, het tegelijk spionage door de Duitse inlichtingendiensten gemakkelijker maakt[31].

De clouddiscussie wordt in Duitsland al enkele jaren gevoerd. In 2011 maakte Duitse minister van Binnenlandse Zaken Hans-Peter Friedrich zich sterk voor een *Bundescloud*, die ervoor zou moeten zorgen dat gevoelige overheids- en bedrijfsgegevens veilig en beschermd tegen spionage opgeslagen worden[32]. Dit heeft vervolg gekregen in de vorm van het consortium *Deutsche Wolke*, waarin een groep Duitse of in Duitsland gevestigde bedrijven samenwerken om een “Made in Germany”-cloud te realiseren. Dit initiatief is gericht op het verminderen van de afhankelijkheid van cloudleveranciers van buiten Duitsland en Europa, waarbij het niet volledig te controleren is waar data wordt opgeslagen, hoe deze wordt vervoerd en gebruikt en of deze beschermd is naar de aard van de wet. Deutsche Wolke streeft ernaar om clouddiensten te leveren die voldoen aan het striktere datasecuritybeleid in Duitsland, waarbij data binnen de landsgrenzen blijft opgeslagen en de dienstverlening transparanter is over waar data is opgeslagen en wat ermee gebeurt bij verplaatsing of verwijdering[33]. Het Duitse Ministerie van Economie en Technologie heeft daarnaast 50 miljoen euro besteed aan subsidie voor innovatieve cloud projecten in het programma *Trusted Cloud*,

---

[29] Merkel, Hollande to discuss European communication network avoiding U.S., Reuters, februari 2014, http://www.reuters.com/article/2014/02/15/us-germany-france-idUSBREA1E0IG20140215.

[30] http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spying-a-933013.html.

[31] http://www.dw.de/deutsche-telekom-plans-for-a-national-internet/a-17171714.

[32] *Innenminister Friedrich will Bundes-Cloud aufbauen,* Witschafts Woche, 17 december 2011.

[33] *Deutsche Wolke - From the Initiative to the Showcase,* website Deutsche Wolke, 19 augustus 2014, http://www.deutsche-wolke.de/index.php?option=com_content&view=article&id=17.

waarin onderzoek is opgenomen naar middelen om clouddiensten tegen interne en externe aanvallen en misbruik te beveiligen[34]. Daarnaast werkt men aan wettelijke raamwerken voor cloud computing rond onderwerpen als privacy, certificering en aansprakelijkheid[35]. Duitsland bundelt dergelijke initiatieven richting 2015 in een "Action Programme on Cloud Computing".

3.1.2. BRICS-landen verbinden elkaar met onderzeese kabel

In september 2013 kwam nieuws naar buiten over mogelijke economische spionage van de Verenigde Staten in Brazilië, waar ook de president van Brazilië zou zijn afgeluisterd[36]. Kort daarna maakte de president bekend dat Brazilië meer vaart gaat maken met de ontwikkeling van de BRICS kabel, een intercontinentale onderzeese verbinding tussen de BRICS-landen Brazilië, Rusland, India, China en Zuid-Afrika. Dit project zou aanvankelijk de BRICS-landen met de Verenigde Staten verbinden[37]. In een herziene aankondiging in 2013 werd echter de nadruk gelegd op de BRICS-kabel als een wereldwijde internetinfrastructuur, onafhankelijk van de Verenigde Staten. Het zou alle delen van de internetinfrastructuur daar overslaan, hetgeen het netwerk minder kwetsbaar zou maken voor spionageactiviteiten en in feite een BRICS-intranet zou creëren. In de originele plannen is desondanks een verbindingspunt in de Verenigde Staten opgenomen. De kosten voor het aanleggen van de 34.000 kilometer BRICS-kabel worden geschat tussen de $750 miljoen[38] en $1,5 miljard[39].

In november 2013 presenteerde de Braziliaanse president eveneens een wetsvoorstel dat internetbedrijven zou verbieden data over Braziliaanse staatsburgers buiten de landsgrenzen op te slaan[40]. Het wetsvoorstel, de Marco Civil da Internet was al sinds 2009 in de maak en werd door de Snowden-onthullingen in april 2014 versneld bekrachtigd. De wet omvat onder andere bescherming van persoonsgegevens. Na veel oppositie werd het controversiële onderdeel dat internetbedrijven verplichtte data uit Brazilië in Brazilië op te slaan, uit het wetsvoorstel geschrapt. In plaats daarvan hebben de wetgevers bepalingen opgenomen die de privacyrechten van Braziliaanse staatsburgers buiten de landsgrenzen moeten verstevigen, zodat hun data beschermd wordt los van waar in de wereld deze is opgeslagen of wordt verwerkt. In het kader van dit onderzoek is niet nader onderzocht of dit inderdaad in de praktijk voldoende bescherming kan bieden.

3.1.3. Zweden en Noorwegen buigen zich over clouddiensten

In juni 2013 hebben Zweedse toezichthouders overeenkomsten tussen de gemeente Salem en Google voor het afnemen van Google Apps clouddiensten afgewezen. De overeenkomst met Google zou Zweden's Personal Data Act schenden en moest worden aangepast of beëindigd. De overeenkomst gaf Google naar verluid teveel vrijheid om persoonsgegevens voor eigen doeleinden te verwerken. Bovendien was onduidelijk wat er met de opgeslagen persoonsgegevens zou gebeuren na afloop van het contract[41].

In Noorwegen heeft een vergelijkbare discussie gewoed over het gebruik van onder andere Google Apps door Noorse gemeenten. De toezichthouder bescherming persoonsgegevens vreesde dat de Patriot Act de bescherming uit de 2000 US-EU Safe Harbor Agreement teniet zou doen. Google heeft uiteindelijk aanpassingen gedaan aan zijn dienstverlening om toe te kunnen zeggen dat data alleen verwerkt zou worden in de specifieke, 'safe harbor' gecertificeerde data centers in de VS, en in de EU/EEA, waar Europese privacy regelgeving van kracht is, conform Noorse wetgeving. Hoewel het daarmee volgens de Noorse Data Protection Commissioner "niet een perfecte oplossing is, voldoet het zo wel aan Noorse wetgeving"[42]. Deze toestemming houdt verder de beperking in dat de gemeenten

---

[34] *Staat fördert innovative Cloud-Projekte mit 50 Millionen Euro*, Cloud Computing Insider, 11 ma.art 2011, http://www.cloudcomputing-insider.de/plattformen/technologien/articles/306734/.
[35] *Rechtsrahmen des Cloud Computing,* Trusted Cloud, 19 augustus 2014, http://www.trusted-cloud.de/560.php.
[36] http://www.reuters.com/article/2013/09/02/us-usa-security-brazil-mexico-idUSBRE9810B620130902.
[37] http://www.ihs.com/products/global-insight/industry-economic-report.aspx?id=1065966716.
[38] *BRICS' $1.2-billion cable project remains a pipe dream,* financialexpress.com, 25 maart 2013.
[39] *Investors mull $1.5 billion undersea cable for BRICS nations*, Reuters, 4 juni 2012, http://www.reuters.com/article/2012/06/04/net-us-safrica-brics-cable-idUSBRE8530SJ20120604.
[40] http://thebricspost.com/brazils-new-internet-bill-to-affect-google-facebook/#.UvxjtfldVsI, The BRICS Post, 6 november 2013.
[41] http://www.datainspektionen.se/press/nyheter/2013/fortsatt-nej-for-kommun-att-anvanda-molntjanst/ , 10 juni 2013.
[42] http://www.computerworld.com/s/article/9231738/Norway_ends_nine_month_ban_on_Google_Apps_use.

Google Apps mogen gebruiken om communicatie tussen personeel en andere autoriteiten te verwerken, maar verbiedt het gebruiken van Google Apps om persoonsgegevens over staatsburgers te verwerken[43]. De Noorse toezichthouder benadrukte dat het gebruik van cloud computing diensten onderhevig is aan voorwaarden en een grondige risicoanalyse. De toezichthouder heeft gemeenten gevraagd om een gedetailleerd verslag van Google's security beleid, een beschrijving van de architectuur van hun informatiesysteem en de fysieke locatie, informatie over hoe Google back-ups doet, wie toegang heeft tot de gegevens evenals uitleg over hoe lokale autoriteiten audits op de beveiliging van Google zouden uitvoeren[44].

3.1.4. Canada beveiligt ICT met een overheidscloud, lokale gegevensopslag en eigendomsbeperkingen

Canada voegt momenteel 485 datacenters van de overheid die verspreid staan over het land samen tot zeven datacenters[45]. Dit moet leiden tot reductie van kosten, toename in capaciteit, modernisering van dienstverlening en een verbetering van de fysieke en digitale veiligheid doordat het aantal kwetsbare punten vermindert. Canada wil hiermee inspelen op toekomstige eisen aan netwerk-, opslag- en rekencapaciteit om met grote hoeveelheden data om te gaan. Het Canadese consolidatie-initiatief is gericht op overheidsdiensten. Het faciliteren of waarborgen van andere vitale sectoren valt buiten de scope. De Canadese overheidscloud is daarmee vergelijkbaar met het Nederlandse initiatief rond de Rijkscloud, waarin bestaande datacenters worden samengevoegd. In Canada hebben zeer kritieke overheidsdiensten zoals die van defensie en binnenlandse veiligheidsdiensten een eigen netwerkinfrastructuur en eigen apparatuur, gescheiden van de te bouwen overheidscloud. Ook heeft Canada in Compute Canada een hoge capaciteit computernetwerk voor onderzoeksdoeleinden, dat los staat van het consolidatie-initiatief[46].

Canada legt nadruk op de veiligheid van gegevens in bewaring van overheidsinstanties (in Canada's cybersecurity strategie[47] omschreven als een van de drie pilaren: "securing government systems"). Twee Canadese provincies, British Columbia en Nova Scotia, hebben verplicht dat gevoelige informatie in bewaring van een overheidsinstantie alleen in Canada mag worden opgeslagen en toegankelijk mag zijn, tenzij enkele uitzonderingen van toepassing zijn[48]. Daarnaast heeft Canada in het aanbestedingstraject voor een nieuw overheidsplatform voor e-mail[49] als vereiste opgenomen dat leveranciers data niet buiten Canada mogen opslaan. Dit beperkt de toegang van buitenlandse partijen tot de Canadese markt. De vraag blijft of deze maatregel effectief is zonder aanvullende maatregelen. Canadese internetproviders maken gebruik van internet exchanges in de Verenigde Staten, waardoor informatie alsnog over netwerken in Verenigde Staten reist alvorens terug te keren in Canada[50]. In de praktijk kan dit dus inhouden dat e-mails tussen Canadese overheden alsnog door de Verenigde Staten gerouteerd worden alvorens in Canada te worden opgeslagen.

Canada hanteert verder een limiet van 46,7 procent op buitenlands eigendom van bepaalde telecommunicatienetwerken[51]. Bovendien vereist Canada dat minstens 80 procent van de leden van de raad van bestuur van telecommunicatienetwerkdiensten uit Canadese burgers bestaat[52].

---

43 Notification of decision – New e-mail solution within Narvik local authority (Narvik kommune) – Google Apps, Norwegian Data Inspectorate, 16 januari 2012.

44 http://www.zdnet.com/no-personal-data-on-google-apps-norway-tells-its-councils-as-it-clears-cloud-use-7000004904/.

45 Data Centre Consolidation, Government of Canada, 11 augustus 2013, via http://www.ssc-spc.gc.ca/pages/dc-cd-eng.html.

46 Strategic Plan 2014-2019, Compute Canada, juni 2014.

47 *Canada's Cyber Security Strategy*, Government of Canada, 2010.

48 Het is in de context van dit onderzoek (nog) niet achterhaald hoe dit gegarandeerd wordt.

49 E-mail Transformation Initiative, Government of Canada, 15, via http://www.ssc-spc.gc.ca/pages/ml-crrl-eng.html.

50 *Towards efficiencies in Canadian Internet Traffic Exchange*, Edelman, Benjamin G., and Bill Woodcock, Canadian Internet Registration Authority, september 2012.

51 *National Trade Estimate Report on foreign trade barriers*, United States Trade representative, maart 2014.

52 De Minister van Economische Zaken gaat in een brief aan de Tweede Kamer (Verwerven van overwegende zeggenschap in een telecommunicatiebedrijf…) in op aanvullende voorzieningen die in Nederland nodig zijn bij overname van een telecommunicatiebedrijf als KPN.

3.1.5. *Verenigd Koninkrijk kiest voor een pakket maatregelen zonder gescheiden netwerken expliciet te overwegen*

Het Verenigd Koninkrijk maakte in 2010 en 2011 bekend dat het £650 miljoen opzij zou zetten om over een periode van vier jaar cybersecurity capaciteiten te ontwikkelen. Met dat bedrag wordt in een scala aan maatregelen voor het verbeteren van cybersecurity geïnvesteerd. Enkele voorbeelden hiervan zijn[53]:

- ontwikkeling van een baseline voor organisaties om zichzelf te beschermen tegen de meest voorkomende cybersecurity bedreigingen; hiertoe werkt men samen met industrieën over standaarden en richtlijnen;
- opzetten van een nieuw 'Cyber Incident Response Scheme' dat organisaties helpt herstellen van cybersecurity aanvallen;
- een uitgebreidere rol voor het Centrum voor de Bescherming van Nationale Infrastructuur rond het beschermen van de Britse kritische systemen en intellectueel eigendom.

Uit de volledige lijst met maatregelen uit de nationale cybersecurity strategie van het Verenigd Koninkrijk blijkt dat men zowel investeert in preventie van cybersecurity risico's door bewustwording, training, technische maatregelen en standaarden. Men investeert echter ook in detectie van incidenten met behulp van een meldpunt en monitoringsdiensten evenals in responscapaciteiten die bepalen hoe te handelen nadat een aanval heeft plaatsgevonden. Het Verenigd Koninkrijk kiest er dan ook voor om pakketten met maatregelen in te zetten om zich tegen cyberdreigingen te weren en neemt gescheiden netwerken niet als afzonderlijk beleidsitem op.

Het Verenigd Koninkrijk heeft onder de noemer "G-Cloud" een centraal platform met een CloudStore[54] opgericht voor de eenvoudige aanbesteding van clouddiensten. De Britse overheid hanteert een cloud first principe, hetgeen inhoudt dat clouddiensten de voorkeur krijgen boven gelijkwaardige niet-cloud gebaseerde oplossingen. Om toegang te krijgen tot het leveren van G-Cloud diensten moeten bedrijven voldoen aan specifieke accrediatie-eisen op zes niveaus. Afhankelijk van het classificatieniveau van gegevens moeten aanbieders van clouddiensten aan striktere eisen voldoen. Sommige marktpartijen gaan zo ver dat ze datacenters in het Verenigd Koninkrijk bouwen zodat ze voldoen aan de accreditatieniveau 's die hen in staat stellen diensten overheidsdiensten te bieden[55]. Vanaf het niveau 4- 'confidential' wordt data opgeslagen in beheer van overheidsdatacenters op beveiligde lokaties.

3.2. *Bestaande gescheiden ICT-netwerken in Nederland*

Er bestaat in Nederland al een aantal ICT-netwerken die in meerdere of mindere mate zijn gescheiden. Tabel 2 toont een - niet-uitputtende - lijst met voorbeelden van gescheiden ICT-netwerken in Nederland.

Tabel 2. Voorbeelden van bestaande gescheiden netwerken in Nederland.

Voorbeeld	Omschrijving
Elektronisch betalings-verkeer	Traditioneel werd elektronisch betalingsverkeer getransporteerd via toegewijde, fysiek gescheiden netwerken (voornamelijk analoge telefoonlijnen of ISDN-D). Sinds enige tijd is het echter ook mogelijk PIN-verkeer over het Internet te transporteren, middels bijvoorbeeld xDSL- of kabelnetwerken. De betaalketen bestaat daarmee uit drie onderdelen: 1. banknetwerken en processoren, 2. openbare telecominfrastructuur en 3. winkelomgeving. Ondernemers kunnen er zelf voor kiezen een redundante verbinding met het bankennetwerk aan te leggen om de beschikbaarheid van PIN-diensten te vergroten[56]. Banken hebben onderling infrastructuren voor het uitwisselen van informatie.

53 https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace.

54 *How to use CloudStore,* Cabinet Office, 1 november 2013 https://www.gov.uk/how-to-use-cloudstore.

55 Oracle targets government cloud deals with new UK datacenter, ZDnet, 13 mei 2014. http://www.zdnet.com/oracle-targets-government-cloud-deals-with-new-uk-datacentre-7000015363/

56 *Analyse robuustheid van het betalingsverkeer, Maatschappelijk Overleg Betalingsverkeer*, 2013.

Entropia Digital	Mobiel bedrijfstelecommunicatie netwerk (op basis van TETRA-technologie) bestemd voor de professionele gebruiker. Door het toepassen van de digitale trunking-techniek is optimaal radioverkeer voor zowel spraak- als datacommunicatie mogelijk tussen mobilofoons en portofoons onderling en naar een centraal punt, de meldkamer. Het Entropia-netwerk is onder andere bruikbaar op evenementen waar het normale mobiele netwerk overbelast is. In 2014 maakte bijvoorbeeld de Nijmeegse Vierdaagse gebruikt van het Entropia-netwerk om beschikbaarheid en privacy voor onderlinge communicatie van de organisatie te verzorgen[57].
Mobitex Netwerk	Met een beschikbaarheid van 99,99% is Mobitex van RAM Mobile Data een radionetwerk gebaseerd op kleine datapaketten dat voldoet aan de eisen die politie, brandweer en vele andere organisaties stellen voor hun bedrijfs- en tijdkritische toepassingen. Het netwerk wordt gebruikt door: politie, brandweer, ambulance, beveiligers van bankfilialen en pinautomaten, Douane, Belastingdienst, waterschappen, ANWB, retailketens[58] en voor toepassingen als taximeters en het uitlezen van parkeermeters.
Alliander	Alliander werkt aan een eigen draadloos telecommunicatienetwerk. Dit CDMA-netwerk (code division multiple access) verzorgt de communicatie met verschillende toepassingen in het energienet, zoals slimme meters, en intelligente middenspanningsruimtes. Het zal echter ook bruikbaar zijn voor Machine-to-Machine (M2M) telecomdiensten als storingsverklikkers, waterstandsensoren en dijkbewaking. Alliander wil het CDMA-netwerk aanbieden aan nutsbedrijven en (semi-)publieke partijen met een kritische infrastructuur die hoge eisen stellen aan de veiligheid en beschikbaarheid van telecommunicatie[59].
GSM-Rail (GSM-R)	GSM-R is een systeem voor radiocommunicatie voor spoorwegen. Via GSM-R worden rijtoestemmingen aan treinen doorgegeven en geven treinen hun positiemeldingen door via een versleutelde verbinding. GSM-R wordt ook ingezet voor reisinformatie op stations. Om te voorkomen dat openbare mobiele netwerken communicatie op het spoor verstoren is er frequentieruimte gereserveerd voor GSM-R. ProRail laat dit netwerk bouwen en beheren door Mobirail, een samenwerking tussen KPN en Nokia Solutions and Networks.
C2000	C2000 is een gesloten mobiel communicatienetwerk en bedoeld voor continu gebruik door de Nederlandse hulp- en veiligheidsdiensten. Hulpverleners kunnen via C2000 met de meldkamer en elkaar communiceren. C2000 is gebaseerd op de wereldwijde TETRA (Terrestrial Trunked Radio) -standaard voor mobiele groepscommunicatie, en maakt daarnaast nog gebruik van het P2000 paging alarmeringsnetwerk en een aantal specifiek voor Nederland ontwikkelde functionele toevoegingen op het radio- en alarmeringssysteem. Het netwerk heeft buitenshuis een landelijke dekking van 97,6% (in 2012) en is erop gericht ook bij zware belasting beschikbaar te blijven. Spraakverkeer over C2000 is versleuteld zodat het moeilijker kan worden afgeluisterd[60]. Het netwerk bestaat uit ongeveer 500 zendmasten (medio 2013) voor het radio netwerk, en maakt deels gebruik van het defensie netwerk NAFIN[61] voor de vaste verbindingen in het kernnetwerk.
Nood Communicatie Voorziening (NCV)	Deze opvolger van het technisch verouderde Nationaal Noodnet, in gebruik door overheid, hulpdiensten en vitale sectoren, moet voorkomen dat communicatie stilvalt tijdens een ramp of crisis, als reguliere openbare netwerken overbelast raken of uitvallen. Het netwerk is gericht op beschikbaarheid in bijzondere situaties zoals overstromingen, stroomuitval, terrorisme en congestie. Naast spraakverkeer ondersteunt het netwerk ook videoverkeer. Het benodigde dataverkeer is gebaseerd op het internet protocol en verloopt via de spraak- en data infrastructuur van KPN[62], en dus op basis van gedeelde capaciteit op bestaande lijnen. Voor dataverkeer wordt Epacity van KPN gebruikt, een VPN-verbinding waarmee alle vestigingen in het VPN direct met elkaar kunnen communiceren. Het netwerk is gerealiseerd door een samenwerking tussen Logius, dienst Digitale Overheid van het ministerie van BZK en KPN.
Diginetwerk	Diginetwerk verbindt bestaande netwerken van overheidsorganisaties met elkaar, waaronder de Haagse Ring, die op zijn beurt weer als een virtueel gescheiden netwerk op het glasvezelnetwerk van NAFIN draait. Zo ontstaat er een besloten netwerk van overheidsnetwerken[63]. Via Diginetwerk kunnen overheden beveiligd gegevens uitwisselen met andere overheden.

[57] *Vierdaagse zet Tetra-netwerk van Entropia in*, Computable, 15 juli 2014.

[58] *RAM Mobile data, onze diensten*, http://www.ram.nl/onze-diensten/mobitex/, 21 juli 2014.

[59] *CDMA Utilities B.V.*, http://www.alliander.com/nl/alliander/overalliander/bedrijfsprofiel/participaties/cdma.htm, 21 juli 2014.

[60] *Over C2000*, https://www.c2000.nl/, 22 juli 2014.

[61] *Strategisch beheer C2000: kiezen voor slagkracht*, Verdonck, Klooster & Associates (VKA) , Het Expertice Centrum (HEC), WODC, 2011.

[62] *NoodCommunicatieVoorziening*, Intercom, Drs. Ralph Kronieger, Ordina Consult Public, 2013-I.

[63] *Diginetwerk*, http://e-overheid.nl/onderwerpen/voortgang-en-planning/releasekalender/bouwsteen/diginetwerk/product/diginetwerk, 21 juli 2014.

Rijksoverheid-netwerk 2.0 (RON 2.0)	RON2.0 is een gesloten virtueel netwerk voor de Rijksoverheid. Het biedt via standaarden en koppelvlakken connectiviteit tussen overheid, burgers en bedrijven, waarbij gebruik gemaakt wordt van een enkel koppelvlak richting internet. Door consolidatie van koppelvlakken is het mogelijk betere beveiliging te bieden en de weerbaarheid te vergroten. Zo zou in noodsituaties de internetkoppeling eventueel tijdelijk opgeheven kunnen worden. RON2.0 vormt voorts de verbinding met buitenlandse overheden en ketenpartners[64]. RON2.0 vormt samen met de geconsolideerde datacenters het fundament van de generieke ICT-infrastructuur van de Rijksoverheid met respectievelijk connectiviteit, verwerkingscapaciteit en opslagvoorzieningen en vormt daarmee de basis voor de Rijkscloud. Voor de netwerkconnectiviteit worden generieke, rijksbrede (technische) kaders opgesteld op basis waarvan een samenhangend netwerk van netwerken zal worden gerealiseerd als generieke ICT-voorziening voor de rijksoverheid waarin interoperabiliteit is gewaarborgd. Kostenbesparing en adequate informatiebeveiliging zijn hierbij belangrijke doelen. De wijze waarop RON2.0/Rijkscloud wordt gebouwd is mede afhankelijk van de definitieve Rijksbrede sourcingsstrategie. Een verkenning voor een deel hiervan (backbone, en dus koppeling tussen Rijksdatacenters) is al uitgevoerd. Er zijn echter nog geen bestuurlijke besluiten voor de lange termijn genomen.
CloudNL	KPN biedt CloudNL haar klanten naar eigen zeggen een “volledig Nederlandse cloud”. CloudNL wordt vanuit Nederland beheerd en draait in Nederlandse datacenters. KPN verzekert dat klanten met CloudNL voldoen aan de voor hun branche geldende wet- en regelgeving. Dit wordt gerealiseerd door het toepassen van een Cloud Compliance Framework[65].
Netherlands Armed Forces Integrated Network (NAFIN)	NAFIN is het fysiek gescheiden en beveiligd glasvezelnetwerk van het Nederlands Ministerie van Defensie[66]. Het netwerk is beveiligd door kabels die moeilijk zijn af te tappen en fysiek moeilijk benaderbaar wegens door militairen beschermde infrastructuur[67]. Inmiddels wordt NAFIN ook gebruikt om andere overheidsdiensten op te leveren, zoals de Haagse Ring[68].
Rijkswaterstaat	Rijkswaterstaat heeft glasvezelkabels langs snelwegen ter aansturing van de matrixborden die verkeersinformatie weergeven. Daarnaast gebruikt Rijkswaterstaat glasvezelnetwerken voor andere toepassingen, bijvoorbeeld tussen de stuwcomplexen van Hagestein, Amerongen en Driel om deze in de toekomst op afstand vanaf één centrale locatie te bedienen voor een efficiëntere inzet van personeel[69].
TenneT	Tennet heeft een groot aantal hoogspanningsstations verbonden met een glasvezelnetwerk voor de communicatie tussen diverse hoogspanningsstations, het bedrijfsvoeringcentrum en camerabeelden voor de meldkamer[70].

Uit bovenstaande voorbeelden blijkt dat Nederland niet vanuit een ‘Greenfield’-situatie start wat betreft gescheiden netwerken. Veel van de genoemde netwerken bestaan al langere tijd. Zo is het glasvezelnetwerk voor NAFIN in 1996 opgeleverd door de toenmalige PTT en is C2000 sinds 2004 operationeel[71]. Deze gescheiden netwerken zijn daarmee geen reactie op de Snowden-onthullingen of de DDoS-aanvallen op Nederlandse banken in 2013 maar een oplossing voor specifieke problemen of behoeften zoals ontbrekende functionaliteit, hoge beschikbaarheid, lagere kosten en/of hoge vertrouwelijkheid.

Daarnaast blijkt dat bepaalde vitale sectoren, zoals de financiële sector of de energiesector, zonder overheidsinterventie voldoende geprikkeld zijn om gescheiden ICT-infrastructuren aan te leggen. Dit kan bijvoorbeeld op basis van huurlijnen, waarbij überhaupt geen betrokkenheid van de overheid noodzakelijk is. Bij verdere fysieke scheiding is wel toestemming van de overheid nodig om een gescheiden netwerk te realiseren, bijvoorbeeld voor het verkrijgen van graafrechten of het verwerven van spectrum.

---

64 *Rijksoverheidsnetwerk 2.0, en netwerk van netwerken*, Alexander Hielkema (Logius) en Leon-Paul de Rouw (DGOBR/DIR), 27 juni 2013.

65 *CloudNL, de Nederlandse cloud van KPN,* KPN, 19 augustus 2014 http://www.kpn.com/itsolutions/themas/cloud/cloudnl.htm.

66 Wikipedia, august 2013.

67 *DTO automatiseringsspil voor alle krijgsmachtsonderdelen*, Computable, 30 augustus 2002 http://www.computable.nl/artikel/praktijk/overheid/1332398/1277202/dto-automatiseringsspil-voor-alle-krijgsmachtsonderdelen.html.

68 *Uitbesteding DTO*, kamerbrief 10 november 2005.

69 *Glasvezel stuwenseble*, Compass, http://www.compass.nl/glasvezel-stuwensemble, 21 juli 2014/.

70 *Aanleg glasvezel naar 279 hoogspanningsstations*, VolkerWessels, 21 maart 2013.

71 *Over C2000*, https://www.c2000.nl/, 22 juli 2014.

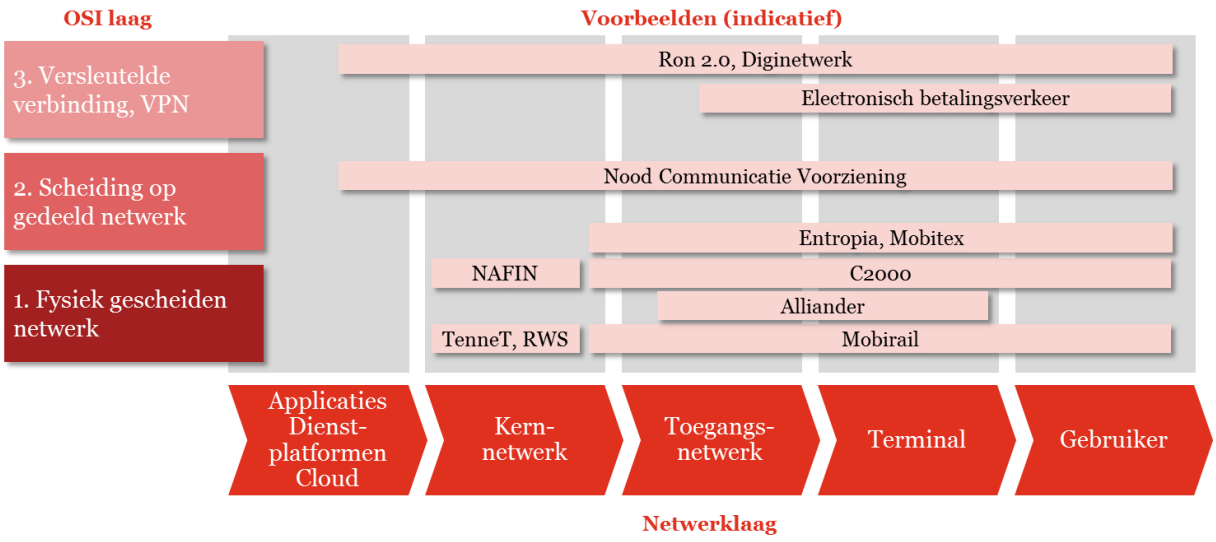
De beschreven netwerken zijn op verschillende wijze gescheiden - in de productieketen, op netwerkniveau en/of op fysieke of virtuele wijze - als voortvloeisel van verschillende afwegingen op het gebied van technische interoperabiliteit, functionaliteit, veiligheid, kosten, en wetgeving. Terwijl het NAFIN netwerk fysiek gescheiden is, maakt het betalingsverkeer deels gebruik van versleutelde informatie over het reguliere internet.

4. **Bevindingen:** *de haalbaarheid van volledige scheiding is twijfelachtig, wenselijkheid moet beoordeeld worden in relatie tot alternatieve maatregelen*

In paragraaf 2.3 is toegelicht dat we netwerkscheiding kunnen onderscheiden in ketenscheiding, netwerkhiërarchie-scheiding en fysieke versus virtuele scheiding. Op basis van deze drie verschillende perspectieven kunnen we de bestaande gescheiden ICT-netwerken in Nederland uit paragraaf 3.2 kenschetsen.

Figuur 5 plaatst hiertoe twee vormen van scheiding in een matrix: scheiding in de verschillende OSI-lagen tegenover scheiding in verschillende netwerkhiërachische niveau's. Zoals in paragraaf 2.3.2 beschreven dient, haaks op bovenstaande perspectieven, ook de productieketen in ogenschouw genomen te worden. Langs dat perspectief blijkt dat de in figuur 5 genoemde netwerken over het algemeen alleen ten aanzien van netwerkgebruik en netwerkbeheer gescheiden zijn. De stappen ontwerp tot en met bouw zijn over het algemeen aan (internationale) marktpartijen uitbesteed, en daarmee onderhevig aan de risico's die in Figuur 2 benoemd worden.

Uit deze matrix blijkt dus dat bij geen van de genoemde bestaande gescheiden netwerken sprake is van een *volledige* scheiding. Een *volledig* gescheiden netwerk zou immers van de bovenste tot de laagste OSI-laag (fysieke scheiding), langs de gehele netwerk-hiërarchie (van gescheiden applicaties/dienst/cloud, tot en met de geautoriseerde gebruiker) evenals door de gehele productieketen gescheiden moeten zijn.



Figuur 5. Indicatieve kenschetsing van aantal bestaande gescheiden ICT-netwerken, naar fysieke versus virtuele laag en netwerk hiërarchisch niveau.

Dit hoofdstuk gaat nader in op kwetsbaarheden van *deels* gescheiden netwerken, evenals de haalbaarheid en wenselijkheid van *volledige* netwerkscheiding, en bespreekt daartoe het vermogen van gescheiden netwerken om dreigingen weg te nemen in het licht van aanvullende of alternatieve oplossingen. Daarnaast staan we stil bij de rol van de overheid in het scheiden van ICT-netwerken.

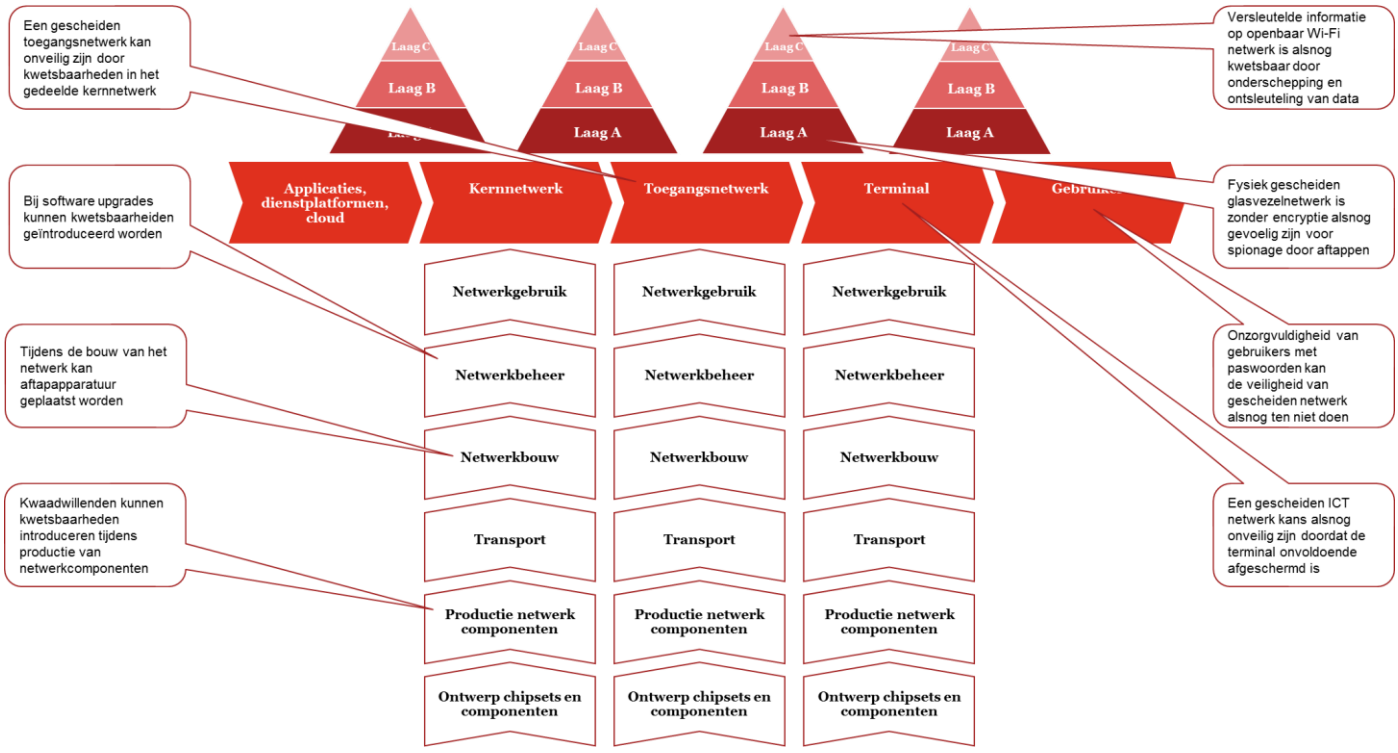
4.1. Onvolledige scheiding neemt een aantal kwetsbaarheden niet weg

In vergelijking tot volledige scheiding van netwerken hebben deels gescheiden netwerken een aantal kwetsbaarheden. Dit kan geïllustreerd worden aan de hand van de volgende voorbeelden:

- Een versleutelde verbinding over een netwerk dat fysiek niet gescheiden is, biedt weliswaar bescherming van integriteit en vertrouwelijkheid, maar is net zo gevoelig voor fysieke verstoring als elke andere dienst over datzelfde netwerk, hetgeen risico's vormt voor de beschikbaarheid.
- Een verbinding over een gescheiden toegangsnetwerk, bijvoorbeeld op basis van eigen mobiele frequenties, zal net zo gevoelig zijn voor kwetsbaarheden in het kernnetwerk als elke andere dienst die gebruik maakt van datzelfde kernnetwerk.
- Een verbinding over een netwerk dat in eigen beheer is, gebouwd door een vertrouwde partij, en voor eigen, geautoriseerde medewerkers, zal net zo gevoelig zijn voor kwetsbaarheid die tijdens de productie van netwerkcomponenten geïntroduceerd zijn, als een ander vergelijkbaar netwerk. Voor een cloud dienst kunnen dreigingen in de keten van ontwerp tot in gebruik name eveneens optreden in de hardware in servers waar cloud computing diensten op draaien, in de netwerkapparatuur die datacenters verbindt, of in de software waarop clouddiensten draaien. Bovendien blijven de terminals en toegangsnetwerken waarmee gebruikers toegang krijgen tot clouddiensten kwetsbaar.

Dit neemt niet weg dat gedeeltelijke scheiding ook sommige kwetsbaarheden kan ondervangen, en daarmee een bijdrage kan leveren aan het verbeteren van de cybersecurity.

Figuur 6 geeft een beeld van de complexiteit van het vraagstuk van gescheiden ICT-netwerken.



Figuur 6. Overzicht van de verschillende perspectieven, inclusief voorbeelden van mogelijke kwetsbaarheden.

4.2. De haalbaarheid van een volledig gescheiden ICT-netwerk is zeer twijfelachtig

Bovenstaande kan aanleiding geven tot de wens om een gescheiden ICT-netwerk aan te leggen dat langs alle genoemde perspectieven (productieketen, hiërarchie en fysiek versus virtueel) *volledig* gescheiden is. Er zijn echter verschillende redenen om aan te nemen dat dit in veel situaties niet haalbaar is:

- **Hoge kosten**: een fysieke gescheiden infrastructuur, langs alle hiërarchische niveaus, waarbij gebruik gemaakt wordt van een volledig vertrouwde productieketen, zal zeer kostbaar zijn. Met name de aanleg van een gescheiden, eigen toegangsnetwerk, vergt een grote investering in geulen en kabels, of antennes en frequenties. Ter illustratie: de initiële investeringskosten die gemoeid waren met het C2000 netwerk bedroegen 765 miljoen[72]. Dit is echter een netwerk dat niet langs alle genoemde perspectieven volledig gescheiden is. Bovendien zijn in deze kosteninventarisatie niet alle maatschappelijke kosten meegenomen. Men zou daar bijvoorbeeld ook rekening moeten houden met de waarde van het gebruikte spectrum. Ook betrof het slechts een mobiel netwerk, waarvan de investeringen ten behoeve van het toegangsnetwerk ten opzichte van een vast toegangsnetwerk relatief beperkt zijn doordat graafwerkzaamheden niet nodig zijn.
- **Beperktere functionele mogelijkheden**: een volledig gescheiden netwerk impliceert bovendien dat er geen koppelingen zijn naar andere, mogelijk niet veilige netwerken. Het succes van het Internet illustreert echter de meerwaarde die ontstaat door een netwerk van netwerken. In het gasnet, dat vroeger op basis van eigen verbindingen werd beheerd, hebben internetkoppelingen er bijvoorbeeld voor gezorgd dat het netwerk tegen lagere kosten vanuit Azië gemonitord en onderhouden kan worden. Uit eerdere ervaringen met gescheiden netwerken voor consumenten zoals HetNet van KPN en Minitel van France Telecom blijkt bovendien dat gesloten netwerken uiteindelijk werden voorbijgestreefd door het open Internet, dat een grotere variëteit aan diensten en snellere innovatie biedt.
- **Gebrek aan voldoende kennis**: een organisatie die streeft naar een volledig gescheiden netwerk zal veel eigen ICT-kennis in huis moeten hebben indien zij geen gebruik wil maken van externe toeleveranciers om ketenrisico's te vermijden. Deze benodigde kennis zal veelal niet aanwezig zijn, en ook niet altijd snel op te bouwen zijn, met name niet als de scheiding doorgetrokken wordt tot diep in de productieketen.
- **Schijnveiligheid**: tot slot kan gesteld worden dat het in eigen huis bouwen, beheren en huisvesten van een ICT-netwerk niet per se betekent dat het netwerk veiliger is. Het kan zelfs een schijnveiligheid creëren, waarbij het idee ontstaat dat doordat alles in eigen beheer is, het dus veiliger is. Externe, specialistische bedrijven zijn mogelijk beter in staat om veiligheid daadwerkelijk te garanderen. Bovendien ontstaat er een sterke afhankelijkheid van een enkel netwerk, indien een gescheiden ICT-netwerk wordt gebruikt voor het faciliteren van meerdere vitale processen. Dat kan op zichzelf de impact van veiligheidsrisico's vergroten, en creëert mogelijk een aantrekkelijk doelwit. De kwetsbaarheid van zelfs een (vrijwel) volledig gescheiden ICT-netwerk kan geïllustreerd worden aan de hand van een van de bekende, recente cyberhacks: de sabotage van nucleaire centrifuges in Iran in 2010, door middel van het programma Stuxnet, een worm die bepaalde Siemens-apparatuur op schadelijke wijze beïnvloedt. Het netwerk waar de nucleaire centrifuges onderdeel van uitmaakte kon als fysiek gescheiden netwerk gekarakteriseerd worden, op een fysiek beveiligde locatie. Toch was het blijkbaar kwetsbaar, vermoedelijk doordat gebruik gemaakt is van naar binnen gesmokkelde memory sticks.

Bovenstaande redenen ten aanzien van de (on) haalbaarheid dienen echter in relatie tot de potentiële baten (wenselijkheid) van een gescheiden ICT-netwerk bezien te worden. Deze zullen per vitale sector, proces, product en dienst verschillen.

[72] *Rapport Eindevaluatie C2000*, mei 2006.

4.3. De wenselijkheid van een gescheiden netwerk moet beoordeeld worden in relatie tot alternatieve maatregelen op basis van een specifieke risicoanalyse

4.3.1. Een gescheiden ICT-netwerk: slechts één van de mogelijke remedies

De Nationale Cyber Security Strategie 2[73] meldt dat Nederland streeft naar het voorkomen van schade door verstoring, uitval of misbruik van ICT. Het aanleggen van een gescheiden ICT-netwerk of cloud, is slechts één van de maatregelen die zou kunnen bijdragen aan het verbeteren van de cybersecurity van vertrouwelijke (overheids-)data en van vitale diensten. Er zijn vele andere, deels eenvoudigere maatregelen denkbaar die een bijdrage kunnen leveren aan het verbeteren van de cybersecurity. Tabel 3 geeft een aantal voorbeelden van andere maatregelen welke zijn ingedeeld in drie categorieën: preventie van dreigingen, detectie van dreigingen en respons op cybersecurity dreigingen. De ISO27001/2:2013 standaard, een standaard voor informatiebeveiliging, specificeert in meer detail eisen voor de implementatie van beveiligingsmaatregelen.

Tabel 3. Voorbeelden van maatregelen ten behoeve van het verbeteren van de cybersecurity. Bronnen: The Economist 12 juli 2014, project stakeholder sessies 16 en 18 juli 2014.

Maatregel	Beschrijving	Draagt vooral bij aan het verbeteren van:	
Encryptie	Het versleutelen van communicatie en informatie. Edward Snowden benadrukt regelmatig dat “sterke encryptie zelfs de NSA dwarszit”.	Vertrouwelijkheid	Preventie
Authenticatie	Controle op wie recht heeft op toegang en welke toestemmingen daarbij horen, bijvoorbeeld door middel van biometrische identificatie.	Vertrouwelijkheid, integriteit	Preventie
Trainen van werknemers, burgers en consumenten	Werknemers, burgers en consumenten bewust maken van de risico’s, de aanvalstechnieken die gebruikt worden, en de noodzaak van robuuste paswoorden.	Vertrouwelijkheid, integriteit, beschikbaarheid	Preventie
Netwerk monitoring	Complexe algoritmes en wiskundige modellen inzetten om abnormaal gebruik, zoals het opeens downloaden van ongebruikelijk grote datafiles, te detecteren.	Vertrouwelijkheid, integriteit, beschikbaarheid	Detectie
Kennisdeling	Organisaties kunnen een platform opzetten om -snel- kennis te delen over best practices, incidenten, dreigingen, en maatregelen daartegen. In de VS bestaan bijvoorbeeld dergelijke platformen in de retail sector (ISAC, Information Sharing and Analysis Centre), en de financiële sector (FS-ISAC). Het UK Office for Cyber Security and Information Assurance heeft een sector-overstijgend platform opgezet. Het National Institute of Standards and Technology heeft onlangs vrijwillige richtlijnen gepubliceerd voor bedrijven in vitale sectoren zoals energie en transport.	Vertrouwelijkheid, integriteit, beschikbaarheid	Preventie

[73] *De Nationale Cyber Security Strategie 2*, Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Veiligheid en Justitie, 2013.

Veerkracht opbouwen	Aannemende dat het onmogelijk is om alle dreigingen het hoofd te bieden, is het van belang om in geval van een probleem snel te kunnen herstellen. Hiertoe is het hebben van een herstelplan van belang.	Vertrouwelijkheid, integriteit, beschikbaarheid	Respons
Redundantie en koppeling van netwerken	Netwerk operatoren kunnen door eigen redundante netwerkverbindingen, of door het koppelen van hun infrastructuren (zoals bijvoorbeeld middels regionale roaming in geval van mobiele netwerken) in combinatie met routeringsafspraken, er voor zorgen dat er een terugvaloptie is op het moment van een netwerkincident.	Beschikbaarheid	Preventie Respons
Wetgeving	Wet- en regelgeving, bijvoorbeeld om standaarden op te leggen, informatiedeling te stimuleren, of maatregelen af te dwingen. Momenteel stellen bijvoorbeeld de Telecommunicatiewet en de Gaswet al eisen aan de veiligheid van de dienstverlening. Aanbieders van ICT-netwerken en -diensten hebben bijvoorbeeld een zorgplicht tegenover hun klanten.	Vertrouwelijkheid, integriteit, beschikbaarheid	Preventie Respons
Ophaalbruggen	Netwerken die afgeschakeld kunnen worden van het internet of andere delen van het netwerk, indien het internet of de andere delen van het netwerk niet meer worden vertrouwd.	Vertrouwelijkheid, integriteit, beschikbaarheid	Preventie Respons
Certificering, accreditatie en audit	Het bijvoorbeeld op jaarlijkse basis controleren van de processen van operators en leveranciers, door een intern testteam of externe partij. Bijvoorbeeld, in het V.K. is onlangs het Cyber-essentials programma geïntroduceerd, waarbinnen bedrijven een certificaat kunnen aanvragen indien ze aan bepaalde minimum veiligheidseisen voldoen. Dit wordt door middel van een externe controle vastgesteld.	Vertrouwelijkheid, integriteit, beschikbaarheid	Preventie Respons
Verzekeren	Organisaties kunnen zich verzekeren tegen bovenmatige schade door cyberincidenten zoal uitval, verlies of diefstal van digitale assets en online reputatieschade.	Beschikbaarheid, Integriteit, Veiligheid	Preventie Respons

4.3.2. Risicoanalyses zijn nodig om bedreigingen in kaart te brengen en de adequate mitigerende maatregelen te formuleren

In het voorgaande wordt een overzicht geschetst van vele mogelijke dreigingen (hoofdstuk 2.2) evenals mogelijke maatregelen ten behoeve van het verbeteren van de cybersecurity (paragraaf 4.3.1). Bovendien zijn er verschillende vitale producten en diensten (zie appendix B) die elk zeer verschillende eisen kunnen stellen aan de veiligheid van een ICT-netwerk. Maatregelen in het kader van cybersecurity vergen dan ook maatwerk. Gegeven de diversiteit aan producten en diensten, dreigingen en mogelijke maatregelen is het aan te bevelen op basis van een risicoanalyse de risico's, in termen van kans en impact, in kaart te brengen. Hierbij is, zoals de AIVD aangeeft in haar jaarverslag[74], "voor bedrijven en overheden niet alleen zicht op de dreiging van belang,

[74] *Jaarverslag*, Algemene Inlichtingen- en Veiligheidsdienst, 2013.

maar ook kennis van de eigen ICT-systemen, en inzicht in de informatie die beveiligd zou moeten worden (de 'kroonjuwelen')". Ook het rapport Recipe van TNO geeft hiervoor handvatten[75].

Afhankelijk van wat men als acceptabele risico's beschouwt, de inschatting van kans en impact, proportionele mitigerende maatregelen worden geïdentificeerd. Het opzetten van een gescheiden ICT-netwerk zou in sommige situaties een adequate maatregel kunnen zijn. Ook na deze aanpak en implementatie van mitigerende maatregelen, ook van een gescheiden netwerk, blijft gelden dat 100% veiligheid een illusie is. Er zal altijd een (rest)risico zijn, en dus zal een bepaalde risicoacceptatie onvermijdelijk zijn. Een organisatie dient dus vooraf te bepalen welk restrisico ze accepteert, en wat nodig is om risico's te mitigeren.

4.3.3. De rol van de overheid ten aanzien van gescheiden ICT-netwerken is afhankelijk van de belangen die op het spel staan

Om te beoordelen wat de rol van de overheid kan zijn ten aanzien van gescheiden netwerken is het van belang in ogenschouw te nemen welke belangen in onze samenleving geschaad kunnen worden en wat de overheidsverantwoordelijkheid is voor elk van die belangen. Het Cybersecuritybeeld Nederland 4 biedt daartoe een overzicht zoals getoond in Figuur 7. Dit maakt onderscheid tussen individuele belangen, organisatorische belangen, ketenbelangen en maatschappelijke belangen.

Individuele belangen	**Organisatorische belangen**
• Privacy • Vrijheid van meningsuiting • Toegang tot dienstverlening • Fysieke veiligheid	• Producten en diensten • Productiemiddelen (w.o. geld, octrooien) • Reputatie • Vertrouwen
Ketenbelangen	**Maatschappelijke belangen**
• Verantwoordelijkheid voor informatie van burgers of klanten • Beheer van algemene voorzieningen en stelsels, zoals GBA/BRP, iDeal en DigiD • Onderlinge afhankelijkheid tussen organisaties	• Beschikbaarheid van vitale diensten • Bescherming van de (democratische) rechtsorde en nationale veiligheid • Infrastructuur van het internet • Vrij verkeer van diensten • Digitale veiligheid

Figuur 7. Overzicht belangen (bron: Cybersecuritybeeld Nederland CSBN-4, Nationaal Cyber Security Centrum).

Ten aanzien van **individuele belangen** wordt een zekere mate van cyberhygiëne (het toepassen van basis-veiligheidsvereisten) en eigen verantwoordelijkheid verwacht. Toch ligt daarbij ook bij de overheid een verantwoordelijkheid om in het bijzonder persoonsgegevens te beschermen en fysieke veiligheid van burgers te waarborgen.

Ten aanzien van **organisatorische belangen** is de overheid verantwoordelijk voor de veiligheid van haar eigen dienstverlening aan burgers en bedrijven. In principe kan men stellen dat bedrijven of sectoren zelf verantwoordelijk zijn voor een veilige ICT-infrastructuur ten behoeve van hun productie en dienstverlening. Ze hebben er ook baat bij om deze productie en dienstverlening ongestoord te laten verlopen, en daarmee hun reputatie bij, en vertrouwen van, (potentiële) klanten in stand te houden. Er kan hierbij echter sprake zijn van een negatieve externaliteit, een vorm van marktfalen. Dit is in algemene zin het geval wanneer de maatschappelijke kosten van een eventueel incident hoger zijn dan de kosten die voor rekening van het bedrijf of de sector zelf komen. In dat geval zal het bedrijf of de sector namelijk een onvoldoende prikkel hebben om een sociaal optimaal investeringsniveau te hanteren. Dit kan het geval zijn bij vitale diensten, bijvoorbeeld de drinkwatervoorziening, waarbij het aannemelijk is dat de maatschappelijke waarde van schoon drinkwater aanzienlijk hoger is wat tot uiting komt in de rekening aan consumenten. Schoon

[75] *Good Practices manual for CIP policies, Recommended elements of critical infrastructure protection for policy makers in Europe*, TNO, 2011. (https://www.tno.nl/content.cfm?context=uitgelicht&content=uitgelicht_nieuwsbericht&laag1=1229&item_id=2011-09-21%2010:30:22.0).

drinkwater is immers van levensbelang. Een puur commercieel gedreven sector zou in een dergelijk geval maatschappelijk gezien onvoldoende investeren in risico-mitigerende maatregelen.

Ten aanzien van **ketenbelangen** kan men in principe de verantwoordelijkheid bij de markt laten. Door middel van sectorale of cross-sectorale afstemmingen kunnen bedrijven zelf hun verantwoordelijkheid nemen. In de werksessie, waaraan vertegenwoordigers van verschillende sectoren deelnamen, kwam echter naar voren dat er behoefte is aan een initiërende, coördinerende rol van de overheid. De overheid is bij uitstek goed gepositioneerd om verschillende bedrijven of sectoren bij elkaar te brengen, en onderlinge kennisuitwisseling en coördinatie tot stand te brengen.

De overheid dient de **maatschappelijke belangen** te waarborgen. Deze komen in het geding als sprake is van bovengenoemde negatieve externaliteiten, of de democratische rechtsorde of de nationale veiligheid in het geding zijn. In deze gevallen is er dus een duidelijke rol voor de overheid in het waarborgen van cybersecurity, al dan niet middels het bieden van een gescheiden ICT-netwerk.

5. Conclusie

Dit rapport komt tegemoet aan een toezegging uit de *Nationale Cyber Security Strategie 2* (NCSS-2):

"Er wordt een verkenning uitgevoerd in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. Met een gescheiden netwerk nemen de mogelijkheden om de continuïteit van vitale processen te borgen toe. Ook kunnen binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld. Hierdoor kan de privacy/integriteit van de data in deze opslag of cloud worden verbeterd"

De hoofdvraag is daarbij: zijn gescheiden ICT-netwerken in Nederland ***haalbaar*** *en* ***wenselijk***?

Het actiepunt uit het NCSS-2 suggereert een verkenning naar één Nederlands ICT-netwerk voor alle vitale processen en clouddiensten. Volgens de definitie van vitale sectoren door het Ministerie van Binnenlandse Zaken zou dit de sectoren telecommunicatie, drinkwater, energie, voedsel, gezondheid, financieel, keren en beheren oppervlaktewater, rechtsorde, openbaar bestuur, transport evenals de chemische en nucleaire industrie omvatten.

Op basis van de zeer uitgebreide lijst vitale processen, bestaande gescheiden netwerken in Nederland en de bestaande situatie waarin vitale sectoren al over eigen infrastructuur beschikken, concluderen we dat er geen sprake hoeft te zijn van één gescheiden Nederlands netwerk maar dat er sprake kan zijn van meerdere afzonderlijke gescheiden ICT-netwerken naargelang de vitale sector, proces, product of dienst.

Er blijkt bovendien geen eenduidig begrip te zijn voor het begrip *gescheiden netwerk*. We hebben daarom het begrip *volledig gescheiden ICT-netwerk* geïntroduceerd voor een ICT-netwerk dat langs drie perspectieven tot op elke niveau gescheiden is:

1. in de **productieketen**: de keten van ontwerp en assemblage tot netwerkbouw en –beheer;
2. in de **netwerkhiërachie:** van clouddienst en toegangsnetwerk tot lokaal netwerk, apparaten en gebruiker;
3. in het **OSI-model:** van fysieke scheiding en capaciteitsscheiding tot virtuele scheiding en encryptie.

Met betrekking tot de zinsnede in NCSS-2 over het ontwikkelen van een eigen cloud concluderen we dat dit punt al deels wordt geadresseerd door het programma Rijksoverheidnetwerk2.0 (RON2.0) en de Rijkscloud. RON2.0/Rijkscloud biedt veilige connectiviteit, verwerkingscapaciteit en opslagvoorzieningen voor en tussen overheden, burgers en bedrijven. Het programma RON2.0/Rijkscloud is echter specifiek gericht op een breed scala aan diensten binnen de Rijksoverheid en niet op andere overheden of vitale sectoren, hetgeen aansluit bij bovenstaande conclusie over sectorspecifieke cybersecurity oplossingen.

De volgende twee paragrafen beantwoorden de hoofdvraag van het onderzoek.

5.1. Zijn gescheiden ICT-netwerken haalbaar?

Het kan haalbaar zijn om ICT-netwerken *deels* te scheiden op onderdelen van de drie perspectieven productieketen, netwerkhiërarchie en OSI-model. Er bestaan voorbeelden van gescheiden netwerken, zowel in Nederland als in het buitenland. Met name de Nederlandse hulpdiensten beschikken al over deels gescheiden netwerken maar ook in private sectoren zijn er deels gescheiden netwerken. Men kan delen van netwerken op verschillende manieren afschermen. De manier waarop hangt af van de dreiging waartegen bescherming is gewenst, en de mate waarin middelen beschikbaar zijn. Zo kan men de kans op aftappen verkleinen door netwerken fysiek te scheiden en de toegang ertoe geografisch te beperken.

Volledige scheiding van ICT-netwerken van vitale sectoren lijkt echter illusoir. Afhankelijk van de sector, de dienst of het product verschilt de haalbaarheid voor het scheiden van ICT-netwerken uit het oogpunt van technische haalbaarheid, juridische armslag, beschikbare kennis en financiële middelen.

5.1.1. Technische haalbaarheid

Wat betreft technische haalbaarheid is het van belang in acht te nemen dat Nederland niet vanuit een 'greenfield'-situatie start waarin ICT-infrastructuren van de grond af aan worden opgebouwd. In het verleden gemaakte keuzes rond de aanleg van glasvezel, koper, coax, antennemasten, datacentra en andere ICT-infrastructuur bepalen de oplossingsruimte voor het scheiden van netwerken wegens eisen aan interoperabiliteit. Dit is terug te zien in keuzes rond de bestaande gescheiden netwerken in Nederland, die in uiteenlopende mate voortbouwen op bestaande ICT-netwerken.

Een volledig gescheiden *productieketen* kan risico's als ingebouwde *backdoors* (achterdeuren) in ICT verminderen maar daarmee ontzegt Nederland zich toegang tot een internationale markt waarin de laatste kennis op cybersecurity gebied tegen een marktconforme prijs beschikbaar is. Nederland heeft niet alle kennis in huis om van kop tot staart alle aspecten van een ICT-infrastructuur te scheiden. Door naar de ICT-productieketen te kijken, van ontwerp en productie tot levering en gebruik, wordt duidelijk dat de laatste stand der techniek veelal afkomstig is van buitenlandse bedrijven. Bovendien dient men rekening te houden met Nederlands en Europees aanbestedingsrecht. Juridisch gezien zijn er mogelijk obstakels om af te dwingen dat ICT-componenten uitsluitend in Nederland, door Nederlandse bedrijven, worden geproduceerd, beheerd en gebruikt. Zelfs in omstandigheden waar geografische scheiding kan worden afgedwongen, bijvoorbeeld door een clouddatacentrum in Nederland te huisvesten, kan het zo zijn dat de leverancier van de clouddiensten onder buitenlandse wetgeving valt, waardoor buitenlandse inlichtingendiensten alsnog toegang hebben tot deze infrastructuur.

Scheiding in de *netwerkhiërarchie* is haalbaar op het niveau van gebruikers, apparatuur en het toegangsnetwerk tot het Internet, bijvoorbeeld middels huurlijnen. Verdere scheiding in het kernnetwerk en clouddiensten vereist een aanzienlijk grotere inzet van middelen, terwijl er alsnog sprake blijft van restrisico's als dreigingen door interne actoren.

Scheiding in de *OSI-laag* betreft een glijdende schaal van fysieke tot virtuele scheiding. Encryptie is een mogelijk haalbare maatregel en zou een groot aantal risico's met betrekking tot integriteit en vertrouwelijkheid van data kunnen afdekken. Encryptie kan echter als keerzijde hebben dat het extra capaciteit van ICT-voorzieningen vereist waardoor het voor grote hoeveelheden data mogelijk minder bruikbaar is. Verdergaande fysieke scheiding vereist zeer grote investeringen in het aanleggen van kabels, de aanschaf van netwerkapparatuur, verwerving van spectrum enzovoorts.

Uitspraken wat betreft technische haalbaarheid van ICT-scheiding kunnen we voornamelijk doen voor de huidige stand van zaken. De ontwikkelingen in ICT-infrastructuren neigen naar het steeds verder combineren van netwerken tot een *Internet of Things*, waarbij netwerken en apparaten maar ook alledaagse objecten met elkaar verbonden zijn. Snelle ontwikkelingen op dit gebied kunnen tot gevolg hebben dat wat nu een op zichzelf staand netwerk is, in de toekomst onderdeel wordt van een fijnmazig netwerk. Ook bij bestaande gescheiden ICT-netwerken zoals NAFIN is te zien dat er gedurende de levensduur van een ICT-netwerk meer koppelpunten met andere netwerken en het Internet ontstaan, in veel gevallen wegens uitbreiding van functionaliteit maar in andere gevallen ook uit kostenoogpunt. Bedreigingen veranderen over tijd eveneens in aard. De middelen van bedreigende actoren ontwikkelen zich en worden steeds meer gemeengoed waardoor een gescheiden netwerk wellicht geen oplossing is van dreigingen in de nabije toekomst.

5.1.2. Financiële haalbaarheid

Het opzetten van een volledige gescheiden ICT-netwerk zal significante investeringen in kennisopbouw en aanlegkosten vergen. Om de financiële haalbaarheid van gescheiden netwerken te bepalen is echter een kostenanalyse per sector, dienst en product nodig. Zo verschilt per sector de mogelijkheid om de kosten van investeringen in ICT door te rekenen aan de eindgebruiker. Bovendien is er per sector sprake van uiteenlopende typen infrastructuur, met bijbehorende eigenschappen zoals het aantal knooppunten, de dekkingsgraad, de afschrijvingen op bestaande ICT-

infrastructuur enzovoorts. Een uitspraak doen over de financiële haalbaarheid van een gescheiden ICT-infrastructuur vergt bovendien inzicht in wie er verantwoordelijk zou zijn voor het dragen van de kosten van een gescheiden netwerk. Is dit de overheid, zijn dit private partijen is er sprake van publiek-private samenwerking of werkt men wellicht samen in Europees verband? Een uitdaging hierbij is ook het kwantificeren van de baten van gescheiden netwerken. Deze verschillen afhankelijk van wat de drijfveer van de netwerkscheiding is: beschikbaarheid, integriteit of vertrouwelijkheid.

5.2. Zijn gescheiden ICT-netwerken wenselijk?

Alvorens zich af te vragen of men gescheiden ICT-netwerken moet inzetten, dient men allereerst de vraag te stellen: *Hoe kunnen cybersecurity risico's afgewend worden per sector, product of dienst?* Er is namelijk een mix van maatregelen mogelijk om cybersecurity risico's in meer of mindere mate te mitigeren. Om deze vraag te beantwoorden zijn gedegen risicoanalyses nodig, specifiek toegespitst op de sector, product of dienst waar de vraag betrekking op heeft. Het uitvoeren van dergelijke specifieke risicoanalyses ligt buiten de reikwijdte van dit onderzoek. In algemene zin dient de risicoanalyse zich te richten op zaken als:

- wat de belangen in vitale ICT-netwerken en -diensten in Nederland zijn;
- wat de bedreigingen zijn voor deze vitale ICT-netwerken en -diensten;
- wat de weerbaarheid is van deze vitale ICT-netwerken en -diensten;
- in welke mate hier risico's uit voortvloeien voor de beschikbaarheid, integriteit en vertrouwelijkheid van ICT-netwerken en -diensten in Nederland;
- de kans op uitkomst van deze risico's; en
- de impact van deze risico's, kwalitatief en kwantitatief.

In het Cybersecuritybeeld Nederland-4 wordt in kaart gebracht wat bedreigende actoren, hun intenties, vaardigheidsniveau 's en doelwitten zijn. Deze analyse kan verder worden verdiept om de waarschijnlijkheid van risico's te kwantificeren evenals de impact hiervan. Het resultaat van "*waarschijnlijkheid*impact*" geeft vervolgens de omvang van het af te dekken risico af. Hiermee kan men nader bestuderen welke scala van maatregelen efficiënt en effectief in te zetten om cybersecurity risico's te mitigeren. Dit kan een gescheiden netwerk omvatten, maar eveneens zaken als encryptie, verbeteren van toegangscontrole, training van gebruikers, detectie van incidenten, wetgeving, ICT-ophaalbruggen, certificering, accreditatie en audits. Op deze manier kan men de baten- en kostenkant van een gescheiden netwerk in vergelijking met aanvullende en alternatieve maatregelen beter onderbouwen. Een blik op ontwikkelingen in het buitenland laat dan ook zien dat landen als het Verenigd Koninkrijk, Canada en Brazilië investeren in pakketten aan cybersecuritymaatregelen.

De noodzaak om aanvullende en alternatieve maatregelen te overwegen is te illustreren door terug te blikken op twee incidenten die mede de aanleiding hebben gevormd voor dit onderzoek, de DDoS-aanvallen op banken in april 2013 en de Snowden-onthullingen over internationale spionage. Voor verweer tegen DDoS-aanvallen beschikt Nederland inmiddels over een commerciële oplossing in de vorm van De Nationale Anti DDoS Wasstraat (NAWAS). Internationale spionage is mogelijk niet te voorkomen wegens de uitgebreide middelen waar staten over beschikken, met encryptie kan echter de integriteit en vertrouwelijkheid van informatie gewaarborgd worden terwijl de discussie over de reikwijdte van de Patriot Act mogelijk om juridische oplossingen vraagt naast maatregelen rond aanbesteding en geografische afbakening van dataopslag.

De noodzaak om sector- en dienstspecifieke risicoanalyse en evaluatie van maatregelen uit te voeren impliceert dat het niet goed mogelijk is om in *generieke* zin conclusies te trekken ten aanzien van de wenselijkheid van een gescheiden ICT-netwerk, en hoe een dergelijk netwerk vervolgens opgezet zou moeten worden. Dit dient een sector- en dienst-specifieke afweging te zijn van dreiging, belang en kosten van een gescheiden ICT-netwerk versus alternatieve maatregelen.

A. Appendix: bijdragen aan het onderzoek

Vertegenwoordigde organisaties in stuurgroep

Ministerie van Veiligheid en Justitie
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
VNO-NCW - MKB-Nederland
Nederland ICT

In werksessies participerende organisaties

Ministerie van Veiligheid en Justitie
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
VNO-NCW MKB-Nederland
Nederland ICT
Stichting NLnet
Eurofiber
AMS-IX
KPN
Ziggo
Compumatica
Rabobank
ING
Politie
Gasunie

B. Appendix: vitale sectoren en diensten

Onderstaand overzicht van vitale sectoren geeft een overzicht van diensten en producten waarvan voornamelijk de *beschikbaarheid* ofwel *continuïteit* gewaarborgd dient te worden. Er kunnen aanvullend hierop ook andere sectoren en diensten geïdentificeerd worden waarvan de *vertrouwelijkheid* en *integriteit* van groter belang zijn.

Vitale infrastructuren zijn die producten, diensten en processen die, als zij uitvallen, maatschappelijke of economische ontwrichting van (inter-)nationale omvang kunnen veroorzaken, doordat er veel slachtoffers kunnen vallen en/of omdat het herstel zeer lang gaat duren en er geen reële alternatieven voorhanden zijn, terwijl we deze producten en diensten niet kunnen missen. Omdat de gevolgen van de uitval van (delen van de) vitale infrastructuur voor grote delen van de Nederlandse samenleving zeer ernstig kunnen zijn, vergt de bescherming daarvan extra aandacht.

Tabel 4. Overzicht vitale sectoren en diensten (Nationale Risicobeoordeling 2012, Analistennetwerk Nationale Veiligheid, RIVM, 2013).

Sector	Voorbeelden van belangrijke diensten/producten
Energie	• elektriciteit • gas • olie
Telecommunicatie /ICT	• vaste en mobiele telecommunicatievoorziening • radiocommunicatie en navigatie • omroep • internettoegang
Drinkwater	• drinkwatervoorziening
Voedsel	• voedselvoorziening/ veiligheid
Gezondheid	• spoedeisende zorg/ overige ziekenhuiszorg • geneesmiddelen • sera en vaccins
Financieel	• betalingsdiensten/ betalingstructuur • financiële overdracht overheid
Keren en Beheren oppervlaktewater	• beheren waterkwaliteit • keren en beheren waterkwantiteit
Rechtsorde	• rechtspleging en detentie • rechtshandhaving
Openbaar bestuur	• diplomatieke communicatie • informatieverstrekking overheid • krijgsmacht • besluitvorming openbaar bestuur
Transport	• mainport Schiphol • mainport Rotterdam • hoofdwegen- en hoofdvaarwegennet • spoor
Chemische en Nucleaire industrie	• vervoer, opslag en productie/verwerking van chemische en nucleaire stoffen

C. Appendix: het OSI-model

Tabel 5. Volledige OSI-model, en de relatie daarvan met het vereenvoudigde OSI-model zoals dat gehanteerd wordt in dit rapport.

	Data unit	Laag	Functie	Vereenvoudiging
Host lagen	*Data*	7. Toepassingslaag	De gebruikersapplicatie of –toepassing	**Laag C** Virtualisatie/ Encryptie
		6. Presentatielaag	Formatteert en structureert data zodanig dat het lees- of interpreteerbaar is voor de applicatie	
		5. Sessielaag	Start, onderhoudt en beëindigt sessies tussen applicaties	
	Data segment	4. Transportlaag	Segmentatie en volgordelijkheid	
	Datagram	3. Netwerklaag	logische adressering, routeinformatie, foutdetectie en -correctie	
Media Lagen	*Dataframe of 'packet'*	2. Datalink laag	Protocol Multiplexing , Medium toegang en Fysieke addressing (MAC)	**Laag B** Capaciteit
	Bit	1. Fysieke laag	Binaire transmissie, elektrische of optische specificaties van het signaal en fysieke specificaties van het medium	**Laag A** Fysiek