

Zelfs de hersenen zijn voor hackers niet meer veilig

# Uit mijn hoofd

Door ons voor elke pietluttigheid aan te sluiten op internet – je fiets moet immers kunnen praten met je stofzuiger – vergroten we willens en wetens onze onveiligheid. Binnenkort gooien we ook ons denken op het net.

door Malou van Hintum beeld Aart-Jan Venema

**ZE HELPEN MENSEN BIJ HET BESTUREN** van kunstmatige ledematen, een rolstoel of een ander extern apparaat, zoals een tekstverwerker. BCI's (brain-computer interfaces) zijn headsets met elektroden die vastgedrukt op de schedel hersensignalen kunnen opvangen en lezen. Vervolgens sturen ze apparaten buiten onszelf aan. Met dank aan ons wonderbaarlijke brein waarmee we dingen in beweging kunnen zetten door maar aan beweging te denken.

BCI's zijn in eerste instantie ontwikkeld voor patiënten die (deels) verlamd zijn of aan het *locked-in*-syndroom lijden. Maar inmiddels is er in de commerciële, op de consumentenmarkt gerichte wereld grote interesse voor. Zo worden er steeds meer BCI's ontwikkeld voor mensen die computer- en videogames spelen. Die zijn nog lang niet zo accuraat als medische BCI's, maar dat is een kwestie van tijd; onderzoekers en gameontwikkelaars werken hard aan verbeteringen.

In feite zijn BCI's de ultieme vorm van handsfree bediening: in de toekomst hoeven we alleen nog maar te denken wat we willen om het te laten gebeuren. Dat betekent dat straks miljoenen consumenten gebruik maken van apparaten die én continu aan het internet hangen, én rechtstreeks verbonden zijn met hun brein. Voor het gemak, voor de fun, gewoon omdat het kan.

Die voordelen hebben één groot nadeel: deze gebruikers zijn ook miljoenen potentiële targets voor neurocriminel. Zij kunnen deze neurale devices hacken en vervolgens signalen verstoren en kapen; ze kunnen in je hoofd kruipen, je gedrag sturen, je emoties beïnvloeden; ze kunnen je zelfs dodelijk letsel toebrengen. Welkom in de wereld van *brainhacking* en *-jacking*.

Neurocriminel kunnen op twee manieren te werk gaan. Ze kunnen de functies in BCI's beïnvloeden zonder dat hun gebruikers dat willen of weten, en bijvoorbeeld robotarmen saboteren door ruis toe te voegen aan de hersensignalen die de BCI oppikt. Denk bijvoorbeeld aan een arm die in het rond gaat maaien in plaats van een papiertje oppraapt.

Ze kunnen ook daadwerkelijk inbreken in het brein, toonde Ivan Martinovic van Oxford University in 2012 aan. Hij liet in een onderzoeksexperiment zien dat het mogelijk is BCI's te

misbruiken om iemands pincode en creditcardgegevens te kraken, te weten te komen bij welke bank hij klant is, waar hij woont, wanneer hij is geboren en welke mensen hij kent. Dat deed hij door gebruik te maken van P300, een piekje in de hersenactiviteit dat geen mens onder controle heeft en waar ook niemand zich bewust van is.

Hoe gaat dat in zijn werk? De hersenen geven het P300-signaal af als ze iets bekends zien. Martinovic gebruikte P300 door BCI-gebruikers foto's van verschillende geldautomaten te laten zien; zij gaven het P300-signaal af als hun eigen bank in beeld was. Op een vergelijkbare manier achterhaalde hij andere persoonlijke informatie. 'Het gaat hier niet om het direct "aflezen" van specifieke informatie', zegt filosoof en psycholoog Pim Haselager, hoofdonderzoeker bij het Donders Institute for Brain, Cognition and Behaviour in Nijmegen. 'Martinovic gebruikte hersensignalen om gerichter te kunnen raden wat de gezochte informatie is. Zo zit voor tachtig

*adopters* van BCI; het grotere publiek zal volgen met BCI-applicaties voor interactieve televisie en handsfree controlesystemen. Er komen steeds meer commerciële applicaties voor *brainreading* en *brainstimulation* op de markt, zie bijvoorbeeld de producten van het bedrijf Emotiv – *you think, so you can*.

Emotiv moest in 2010 met lede ogen aanzien hoe hacker Cody Brocious de encryptie kraakte van de Emotiv EPOC EEG headset. Deze headset, waar inmiddels al geavanceerdere uitvoeringen van zijn, zet met behulp van sensoren hersensignalen om in een bluetooth- of wifisignaal waardoor je bijvoorbeeld een game kunt spelen, een apparaat kunt besturen zoals een speelgoedautootje of een kleine helikopter, en mentale trainingen kunt doen. Cody wilde de noodzaak van een veiliger ontwerp onder de aandacht brengen; maar wat hij als 'ethische hacker' kan, kan een neurocriminele hacker natuurlijk ook.

Het Amerikaanse leger wil BCI's ontwikke-

## Hacker Barnaby Jack toonde aan dat het mogelijk is iemand een dodelijke schok te geven door een pacemaker te hacken

procent van de gebruikers hun echte bank bij de eerste drie suggesties van het algoritme, duidelijk hoger dan een willekeurige gok. Gekoppeld aan andere informatie die je over die persoon hebt, kan dat interessant zijn.'

Haselager vindt dat je, analoog aan computer-spyware, wel degelijk kunt spreken van 'brain-spyware'. Toch wil hij geen alarmistische boodschap verkondigen. De 'methode Martinovic' is een wel heel heel omslachtige, ruisgevoelige manier om aan persoonlijke gegevens te komen, zegt hij. 'We hebben het ook niet over het meest urgente probleem in de huidige neurotechnologie-wereld. Maar het gaat wel over ontwikkelingen die eraan zitten te komen. Het is daarom goed om nu over dit soort problemen te praten in plaats van later achter de feiten aan te moeten lopen.'

Martinovic bood zijn proefpersonen rechtstreeks plaatjes en getallen aan; in een cybercriminele setting zullen deze, bijvoorbeeld, verstopt zitten in games. Gamers zijn *early*

len om neurale en/of gedragsmatige functies bij frontsoldaten te herstellen en om de training en prestaties van militairen en agenten van de inlichtingendiensten te verbeteren. Je kunt je voorstellen wat er allemaal mis kan gaan als de vijand zijn voordeel gaat doen met veiligheidslekken in die BCI's.

**TOT NU TOE** hadden we het over brainhacking. Van brainjacking is sprake als een hacker het BCI-communicatiekanaal overneemt en daarmee de controle van de gebruiker op de BCI, anders gezegd: de hacker gaat de commando's geven in plaats van de gebruiker.

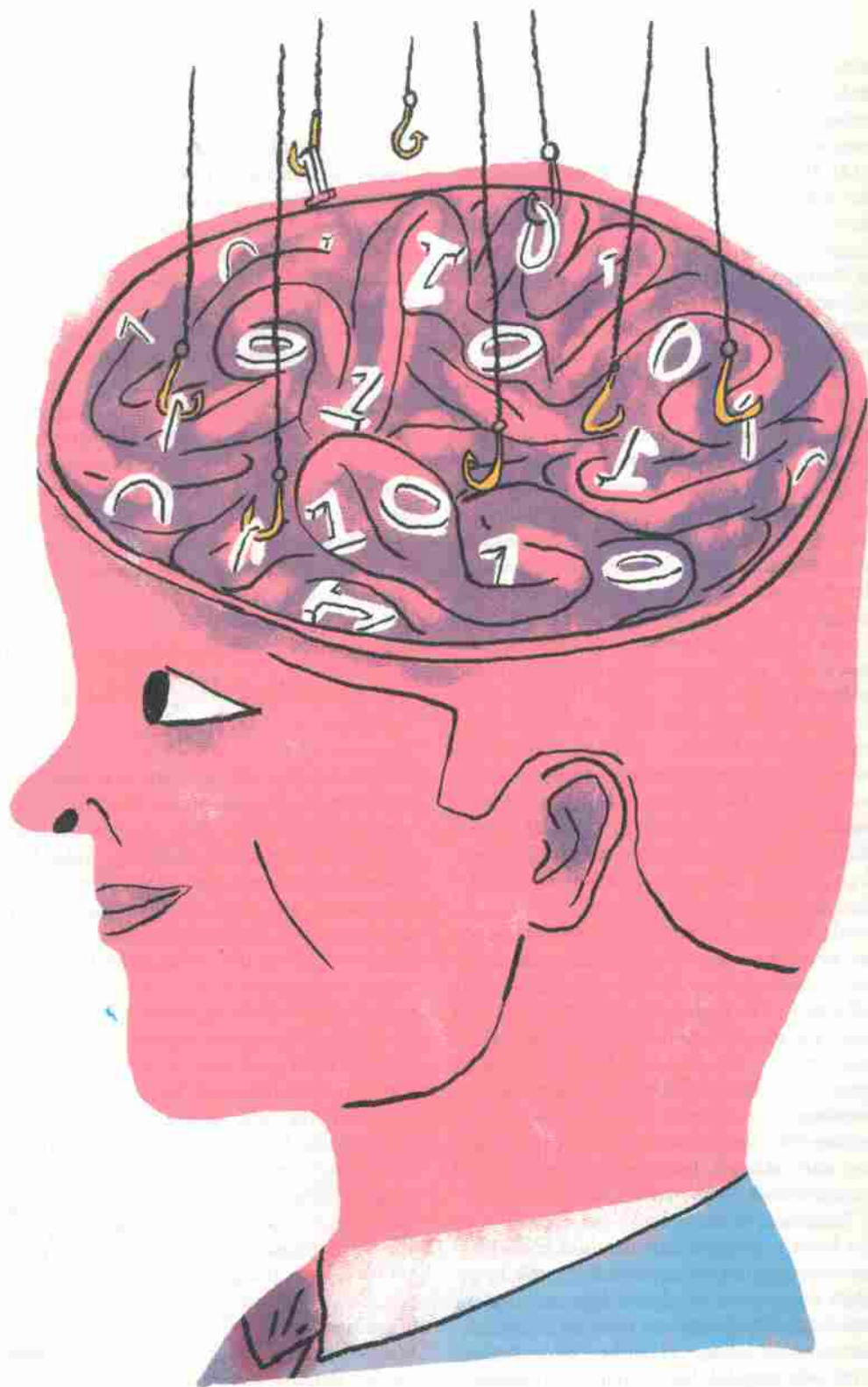
Haselager noemt het voorbeeld van een gefrustreerde hulpverlener die zijn via BCI communicerende patiënt het zwijgen oplegt of die iemand in een rolstoel dwingt om een bepaalde route te nemen. Neurocriminel kunnen bijvoorbeeld ook een BCI-gecontroleerde smartphone hacken en betalingen doen, gevoelige informatie verwijderen of onder de naam van de

gebruiker communiceren met derden. Bovendien kunnen derde partijen schade oplopen. Brainjacking is, kortom, een nieuwe manier om fraude en (identiteits)diefstal te plegen – maar nu doordat neurocriminelen letterlijk in ons hoofd kruipen.

Waarom lopen we deze risico's? Omdat we ons niet op zo'n manier gedragen dat we ze kunnen voorkomen. Neurocriminaliteit is een nieuwe vorm van cybercriminaliteit die we zelf faciliteren omdat we zo ongelooflijk slordig onze gegevens over het world wide web uitstrooien. Inmiddels vertelt de digitale pendant van ons leven in de echte wereld minstens zo veel over onszelf. En dat gebeurt lekker overzichtelijk: op al die met elkaar synchroniserende apparaten vind je al onze gegevens, van paspoortnummer en creditcardcode tot ons favoriete merk koffie, de muziek die we luisteren en de vrienden met wie we omgaan. Foto's, video's, alle apps en websites die we gebruiken, apparaatjes zoals activitytrackers, apps waarop je je psychisch welbevinden bijhoudt en e-readers die weten wat je wanneer in welk tempo en in welke tijdsperiode leest (plus hoe zich dat verhoudt tot andere lezers) maken het beeld compleet. Zelfs je e-mail wordt gescand.

Internet is daarmee een grote snoepwinkel voor overheden en bedrijven, maar ook voor criminelen; een snoepwinkel waarvan de deur wagenwijd openstaat en die elke seconde wordt gevuld met miljoenen data van miljoenen mensen. Dat overheden en bedrijven op basis van die data niet alleen je gedrag in kaart brengen maar ook beïnvloeden en in een bepaalde richting sturen, merken we niet eens. Je hoeft het zelfs niet te merken als cybercriminelen je computer hacken.

Dat wordt anders wanneer die criminelen specifieke data, zoals creditcardgegevens, stelen en je vervolgens geld afhandig maken. De daarop volgende stap in cybercrime, ransomware of cryptoware, is nog ingrijpender: dan kun jijzelf ineens niet meer bij je eigen data omdat je computer gegijzeld wordt door cybercriminelen die dat wel kunnen. Alleen als je betaalt, krijg je weer toegang tot je gegevens – tenminste, dat is wat ze beloven. Die belofte komen ze vaak niet na.



**ONDANKS AL DIE ELLENDE** voelt digitale criminaliteit voor de meeste internetgebruikers niet erg angstaanjagend, misschien omdat ze niet direct fysiek worden bedreigd of mishandeld. Maar hoe lang duurt dat nog? We weten dat draadloze communicatie ons kwetsbaar maakt. Zo worden auto's steeds vaker gestolen omdat criminelen erin slagen de code te onderscheppen – te hacken dus – van de afstandbediening van de autosleutel. Wat met auto's kan, kan ook met allerlei andere apparaten die een slecht beveiligde draadloze regelaar hebben, inclusief medische devices. Al in 2008 voorspelden

onderzoekers dat het mogelijk zou worden een dodelijke aanval uit te voeren op een geïmplanterde ICD (een soort superpacemaker). Niet toevallig werd de draadloze bediening van de ICD van de Amerikaanse oud-vice-president Dick Cheney (2001-2009) uitgeschakeld, uit vrees voor een politieke moord.

Hacker Barnaby Jack liet in 2011 tijdens een conferentie in Las Vegas zien dat het mogelijk is een insulinepomp keer op keer de maximumdosis van 25 eenheden te laten afgeven, totdat het reservoir van driehonderd eenheden helemaal leeg is. Een diabetespatiënt overleeft zo iets

niet. Een jaar later toonde hij op een conferentie in Melbourne aan dat het inderdaad mogelijk is iemand een dodelijke schok te geven door een pacemaker te hacken.

In al deze gevallen moet de hacker zich binnen enkele tientallen meters van zijn slachtoffer bevinden. Maar dat kan in de toekomst best eens niet meer nodig zijn, dankzij het Internet of Things: al die systemen en apparaten die online met elkaar verbonden zijn en die we op grote afstand met behulp van een smartphone kunnen bedienen.

De Britse onderzoeker Laurie Pycroft van Oxford University wijst op de neuroveiligheidsrisico's van breinimplantaten, in het bijzonder Deep Brain Stimulation (DBS).

DBS is een soort 'hersencpacemaker', een onderhuids aangebrachte elektrische stimulator die arts en patiënt samen instellen en die gedoseerd elektronische pulsen afgeeft aan elektroden die op specifieke plekken in de hersenen zijn geïmplantieerd.

DBS is ingrijpend en duur en wordt pas toegepast als parkinsonpatiënten, mensen met epilepsie, Gilles de la Tourette, depressies of dwangstoornissen geen baat meer hebben bij psychotherapieën en/of medicatie. Dankzij DBS kunnen zij de symptomen onderdrukken waarvan ze zoveel last hebben: de epilepticus heeft minder en minder heftige aanvallen, de parkinsonpatiënt heeft minder motorische klachten, degenen met dwang hebben minder dwangklachten, enzovoort.

Als iemand de controle op de instellingen van zo'n apparaatje kan overnemen, kan hij je dingen laten doen en voelen zonder dat je daar zelf iets over te zeggen hebt, aldus Pycroft. Hij beschrijft een – hypothetische – neurocriminele aanval bij DBS die tot mishandeling en zelfs moord kan leiden; doordat neurocriminelen de instellingen veranderen – voltage, frequentie, pulsbreedte (de tijd dat de puls 'aan' is) – waardoor iemand in plaats van veel minder juist veel meer chronische pijn heeft.

Parkinsonpatiënten lopen het risico dat ze niet beter, maar juist helemaal niet meer kunnen bewegen, dat ze hun impulscontrole kwijtraken en manisch worden of hyperseksueel, of pathologisch gaan gokken. Door de veiligheidsnormen voor voltage en pulsbreedte te kraken, is het ook mogelijk hersenweefsel te beschadigen en ernstige handicaps te veroorzaken.

**INMIDDELS WAARSCHUWT** de Amerikaanse FDA (Food and Drug Administration) voor de risico's die patiënten lopen die afhankelijk zijn van slecht beveiligde medische devices. En het Amerikaanse Department of Homeland Security heeft aandacht gevraagd voor de 'onacceptabele risico's' die worden genomen met onveranderbare wachtwoorden in medische apparaten.

Wetenschapper Rinie van Est van TU Eindhoven, (co)auteur van rapporten als *Intieme technologie, Leven als bouw pakket* en *Regels voor het digitale mensenpark*, vindt het vreemd dat medicijnen uit en te na moeten worden

getest voordat ze de markt op mogen, en dat die eis niet aan medische devices wordt gesteld, terwijl dat in feite medische hulpmiddelen zijn die aan dezelfde veiligheidseisen zouden moeten voldoen als medicijnen. Sowieso gelden voor software zelden strenge eisen, met uitzondering voor de vliegtuigindustrie, zegt hij. Een verklaring daarvoor heeft hij ook: 'Op het moment dat we technologie gebruiken om in te grijpen in het lichaam, de biotechnologie, vindt iedereen het normaal om na te denken over ethische issues en moet het allemaal superveilig zijn. Diezelfde gedachte zien we niet bij informatietechnologie. Informatietechnologie hebben we lang gezien als een computer op ons bureau. Maar nu die in de vorm van een gadget of device intieme technologie is geworden, zou dat moeten betekenen dat de eisen die daaraan worden gesteld ook veel hoger worden.'

Maar dat gebeurt niet, laat het voorbeeld van

## DBS zou in de toekomst ook ingezet kunnen worden om abnormaal moreel of gewelddadig gedrag te reguleren

de genetwerkte diabetespatiënten zien. Deze patiënten hadden aanvankelijk een gewone insulinepomp, maar later werden er steeds meer pompen aan het internet gelinkt. In de Rathenau-publicatie *De meetbare mens* staat beschreven wat deze digitalisering betekent: de genetwerkte patiënt die voornamelijk 'data-gedreven zorg' op afstand krijgt, heeft maar heel weinig zicht op wat er nou precies met zijn data gebeurt. Zijn zelfmanagement is dus flink vergroot, maar daar staan nadelen tegenover. *Van Est*: 'Hij heeft geen zicht op welke partijen iets met zijn data doen; hij heeft weinig zeggenschap over die data; hij heeft geen zicht op het moment dat data buiten hem om door derden – wie dan? – worden gedeeld; en hij kan niet zeggen welke data hij wel wil delen en welke niet.' In een papieren dagboek kon dat wel en hoefde zo'n patiënt aan bijvoorbeeld een diabetesverpleegkundige geen uitleg te geven over periodieke lage waarden in de nacht die samenhangen met een specifiek type lichaamsactiviteit. Want die noteerde hij gewoon niet. 'Er is dus een nieuwe datamarkt ontstaan', concludeert Van Est, 'maar is dat in het belang van de patiënt?' Welke belangen spelen er eigenlijk?

**'WAT MIJ VERBAAST**, is dat niemand de vraag stelt *waarom* er altijd een internetconnectie moet zijn.' Technologiefilosof Bibi van den Berg van de Universiteit Leiden gaat in haar artikel *Mind the Air Gap: Preventing Privacy Issues in Robotics* uitgebreid in op het feit dat het zo ontzettend normaal is geworden om altijd en overal maar 'connected' te zijn. Je geldt als een holbewoner als je dat niet bent, als een achterlijke zool als je dat niet wilt.

Alle apparaten die we gebruiken worden uitgerust met een internetaansluiting, zegt ze ter-

wijl op de achtergrond haar stofzuigerrobot aan het werk is. 'Het eerste argument voor het Internet of Things is dat producenten op die manier mensen gepersonaliseerde diensten en informatie kunnen aanleveren. De keerzijde daarvan is dat er ook een stroompje teruggaat naar de producent, namelijk persoonlijke data. Zo kunnen producenten meekijken in het dagelijks leven van consumenten, gedragspatronen analyseren en op basis daarvan profielen maken. Die profielen kunnen ze gebruiken voor *targeted advertising* en prijsdiscriminatie: je krijgt een bepaald product voor een lagere of juist een hogere prijs omdat je, bijvoorbeeld, altijd bepaalde koffiepads gebruikt.' Anders gezegd: de consument krijgt een gepersonaliseerde dienst en betaalt daarvoor met zijn data.

Het tweede argument is volgens Van den Berg 'veel schandaliger': 'Producenten zeggen dat de *time to market* van nieuwe producten

tegenwoordig heel kort is en dat ze zo snel moeten innoveren en nieuwe producten in de markt moeten zetten om te kunnen concurreren dat ze producten moeten verkopen die nog niet helemaal af zijn. De software daarvan is heel erg slecht. Hun redenering is: we bouwen een internetconnectie in en dan kunnen we, terwijl het product al bij de consumenten in huis staat, achter de schermen de software gaan upgraden. Daar hoeft de consument niets van te merken en wij kunnen doorgaan met innoveren.'

Dat maakt die consument dus hartstikke kwetsbaar. Niet voor niets waarschuwt Laurie Pycroft voor de grote neuroveiligheidsrisico's die mensen lopen als hun breinimplantaten in de toekomst mogelijk bediend kunnen worden met smartphones of via internet. Volgens psychiater Damiaan Denys, een van de grootste DBS-specialisten wereldwijd, een onmogelijkheid: 'Programmeren doen wij niet via internet en dat kan ook niet, omdat je een regulator vlak boven de batterij moet houden om instellingen te wijzigen.' Maar kun je zo'n ontwikkeling in een snel innoverende informatiemaatschappij nu al uitsluiten?

Een fundamentele vraag wordt dan belangrijker: waarom willen we eigenlijk met heel ons hebben en houden dag en nacht aan het internet hangen? Waarom is dat zo normaal geworden? 'We zijn met z'n allen in de afdaling beland dat dit de enige manier is waarop het kan', constateert Van den Berg.

De naïeve consument vindt het intussen bovendien erg handig, al die 'slimme apparaten': een smart tv, een slimme energiemeter, een slimme thermostaat, fietsen en koffiezetapparaten met een internetconnectie en ga zo maar door. *Van den Berg*: 'Vroeger kocht je gewoon een *stand alone*-apparaat, maar tegenwoordig

hebben heel veel apparaten een wifimodule. Dat is een kostenkwestie. Voor producenten is het gemakkelijker om het zo te doen in plaats van een gesloten netwerkje te maken. En de consument denkt: o wat handig, ik kan vanuit de trein mijn stofzuiger aan het werk zetten. Weet die veel dat dit wordt gebruikt om slechte software te upgraden. Maar de consument betaalt daarvoor de prijs, want die heeft te maken met een groot risico op veiligheidslekken!

Zitten we als consumenten dus in de val? Nee, want de oplossing is eigenlijk heel eenvoudig en in de wereld van cybersecurity al lang bekend, zegt Van den Berg: je beveiligd een omgeving het best door die niet aan het internet te hangen. 'Natuurlijk kun je ook inbreken op een intern netwerk. Maar voor de meeste consumenten geldt dat problemen op het gebied van veiligheid, privacy en gegevensbescherming

zijn opgelost als ontwerpers zichzelf deze simpele vraag stellen: moet dit product echt aan het internet? Als je het leuk vindt dat jouw koelkast, fiets en stofzuiger met elkaar kunnen praten, kan dat in een gesloten netwerk bij jou thuis. Waarom zou je al die data met de buitenwereld willen delen, met alle risico's van dien?' Bovendien kun je er ook voor kiezen om één keer per week of per maand je gegevens te delen, zegt Van Est. 'Dan is je kwetsbaarheid meteen veel minder. Het gevaar is er alleen op het moment dat die lijn openstaat.'

**MAAR JA, WIE GAAT ZICHZELF** nou willens en wetens van de buitenwereld afsluiten? En dus vergroten we elke dag opnieuw onze onveiligheid, en bedenken we het ene idee na de andere toepassing om onszelf nog kwetsbaarder te maken. Zo bestaan voor DBS grootse plannen. Het zou, behalve voor de huidige patiëntenpopulaties, in de toekomst ook ingezet kunnen worden om abnormaal moreel of gewelddadig gedrag te reguleren en kunnen bijdragen aan de cognitieve verbetering van 'gewone' gezonde mensen – met een beetje fantasie kun je je voorstellen welke puinhoop een kwaadwillende hacker zou kunnen aanrichten als ook DBS aan het internet wordt verbonden.

Dan hebben we het nog niet gehad over tDCS, *transcranial direct current stimulation*: een manier om hersenactiviteit te beïnvloeden met behulp van zwakstroom via twee elektroden die je aan weerszijden van je hoofd plaatst. Voor een paar tientjes en met behulp van een handlei-

ding (gemakkelijk te vinden op internet) bouw je deze lichte hersenstimulator eenvoudig zelf. 'Gebruik van tDCS zou volgens sommige onderzoeken leiden tot een toename van verbale creativiteit', zegt Pim Haselager voorzichtig. 'Dus als je een goede indruk wilt maken tijdens een avondje uit, of een werkstuk moet schrijven. Die dingen zijn vaak te verbinden met smartphones en bepaalde apps. Dat is allemaal nog in ontwikkeling en dat gaat ontzettend groeien. De psychologische effecten daarvan zijn beperkt, maar de schaal waarop het toegepast kan worden, is heel groot.'

Intussen zullen producenten er alles aan doen om ons te laten volharden in ons gedrag, onder het motto dat open lijnen veel gebruiksvriendelijker zijn. En sneller – en dat is precies wat we willen. Ergens op wachten is niet meer van deze tijd. Sommige onderzoekers voorspellen dan ook dat toetsenbord, computermuis, touchscreen en ook stemcommando's zullen worden ingeruild voor BCIs: hersensignalen worden de snelste manier om met computers te communiceren.

Ondernemer Elon Musk, de man achter onder meer Tesla (elektrische auto's), SpaceX (ruimtetransport) en Hyperloop (een soort geavanceerde buizenpost), vertelde eind maart over zijn nieuwste initiatief: Neuralink, een bedrijf dat een 'whole brain interface' gaat ontwikkelen. Het gaat daarbij om een netwerk van heel kleine elektroden dat moet gaan fungeren als een 'natuurlijk' onderdeel van onze hersenen waarmee we direct met het internet kunnen communiceren, met alle apparaten die daarop zijn aangesloten, en met alle mensen die ook zo'n BCI hebben. Onze wensen, hoop, angsten en zorgen hoeven we niet meer uit te spreken om ze te delen; ze denken is al voldoende. Sommigen spreken van een mogelijke neuro-revolutie die niet verandert wat mensen op welke manier doen, maar die verandert wie we zijn. Anderen voorzien nog erg veel hobbels en hindernissen, waarvan het uitvoeren van dure, onnodige en riskante neurochirurgische ingrepen bij gezonde mensen niet de minste is.

Musk is trouwens niet de enige die investeert in innovatieve breintechnologieën. Bryan Johnson, een grote Silicon Valley-ondernemer, heeft honderd miljoen dollar gestoken in Kernel, een onderneming die geavanceerde – maar zeer waarschijnlijk niet-invasieve – neurotools gaat ontwikkelen.

Al deze plannen onderstrepen de noodzaak om te onderzoeken wat de ethische en praktische implicaties (kunnen) zijn van breintechnologie, en deze vragen onophoudelijk te blijven herhalen: wie (en wat) geven we toegang tot ons brein? Wat levert het ons eigenlijk op? Tegen welke prijs? En vooral: welke mogelijkheden bouwen de ontwerpers van dit soort technologieën in zodat we zelf de deur hermetisch kunnen afsluiten voor indringers?

Zulke vragen kun je beter (te) vroeg stellen dan te laat. Anders ziet de toekomst er voor neurocriminelen wel heel erg zonnig uit. ♦

