Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

university of groningen / faculty of science and engineering

Rijksuniversiteit Groningen

Neurale netwerken

De wiskundige verschillen en haar toepassing binnen de Rijksinspectie Digitale Infrastructuur

Afstudeerstage Technische Wiskunde

Auteur:
Lisa Larissa Oosterhof

Studentnummer:
S3032558

Begeleider RDI:
Sjoert Fleurke

Begeleiders RUG:
Henk van Waarde
& Roel Luppes

14 november 2023

Inhoudsopgave

1 Introductie

De Rijksinspectie Digitale Infrastructuur zorgt voor een goed werkende digitale infrastructuur. Deze infrastructuur moet beschikbaar, betrouwbaar, stabiel en veilig zijn. Dit wordt onder andere gedaan door te adviseren over wet- en regelgeving. Daarnaast wordt er onafhankelijk en onpartijdig toezicht gehouden op de huidige wet- en regelgeving. De Rijksinspectie Digitale Infrastructuur, afgekort als RDI, staat dan ook voor een veilig verbonden Nederland [20]. De RDI valt onder het ministerie van Economische Zaken.

Één van de belangrijke aspecten die spelen binnen een veilig verbonden Nederland is het gebruik van artificiële intelligentie. Er is een enorme toename in het gebruik van artificiële intelligentie, afgekort als AI, door bedrijven op allerlei vlakken [11]. Zo wordt er gebruik gemaakt van generatieve AI zoals de welbekende GPT's. Daarnaast is er de afgelopen jaren een toename van slimme apparatuur te zien. Denk hierbij aan telefoons die ons gezicht herkennen, een auto die op de autopilot kan rijden of slimme verlichting die aan gaat als er door een mens iets gezegd wordt [24]. Hier komt de directie apparatuur van de RDI dan ook in beeld.

Op 21 april 2021 is de Artificial Intelligence act voorgesteld door de Europese Unie. De wet- en regelgeving rondom AI zal gereguleerd worden door de AI Act. Het doel is om vanaf 2026 toezicht te houden op artificiële intelligentie. Momenteel wordt er druk overlegd wie de toezichthouder op de verschillende aspecten gaat worden. De RDI graag een toezichthouder worden op het gebied van artificiële intelligentie zodat zij bijvoorbeeld de apparatuur die op de markt komt kan controleren op veilig gebruik van artificiële intelligentie [21].

Naast het feit dat de RDI graag de toezichthouder wil worden voor de AI Act, houdt zij momenteel al toezicht op vertrouwensdiensten die de e-herkenning uitvoeren. Dit betekent dat de RDI toezicht houdt op bedrijven die de koppeling tussen de fysieke en elektronische identiteit maken. Ook in dit vakgebied komt steeds meer artificiële intelligentie terug. Deze AI wordt voornamelijk gebruikt om identiteitsfraude te plegen. Zo worden er door personen *deep fakes* gemaakt zodat een persoon zich kan voordoen als iemand anders. Ook worden de echtheidskenmerken van het identiteitsdocument geprojecteerd op een identiteitsdocument zonder echtheidskenmerken. Dit is een belangrijk onderwerp op het gebied van artificiële intelligentie aangezien dit de veiligheid van burgers en bedrijven in gevaar kan brengen [13].

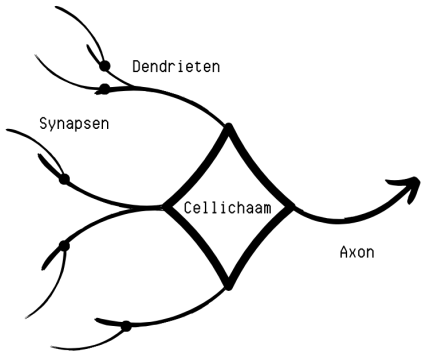
Om Nederland veilig en verbonden te houden zijn er binnen de RDI meerdere groepen die zich bezighouden met de verschillende aspecten van AI. Omdat neurale netwerken momenteel veel gebruikt worden is de wens van de RDI om daar meer kennis over te krijgen. In dit rapport wordt eerst de werking van het menselijk brein en de analogie met neurale netwerken uitgelegd. Hierna worden de wiskundige verschillen van de neurale netwerken uitgelegd. Nadat de wiskundige verschillen zijn uitgediept, is er een marktonderzoek uitgevoerd waarbij er onderzoek is gedaan naar het gebruik van verschillende neurale netwerken. In het laatste hoofdstuk wordt de artificiële intelligentie binnen de RDI besproken.

2 Het menselijk brein

In dit hoofdstuk zal eerst de manier waarop de mens leert worden beschreven. Daarnaast wordt de anatomie van het brein uitgelegd. Hierna wordt de analogie tussen neurale netwerken en de manier waarop de hersenen zijn opgebouwd besproken.

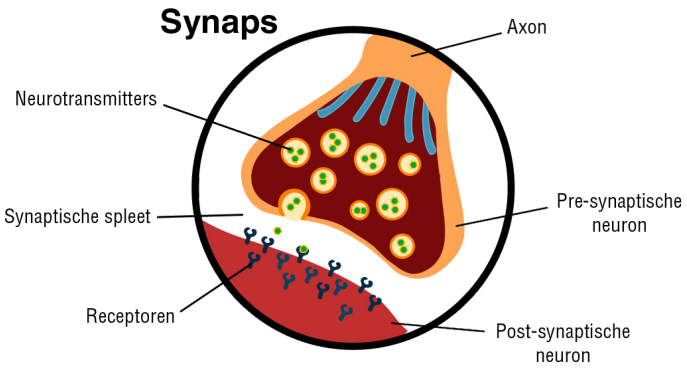
2.1 Leren

In het brein bevinden zich miljarden zenuwcellen. Deze zenuwcellen worden ook wel neuronen genoemd. Door verbindingen tussen deze zenuwcellen te maken leert het brein en door deze verbindingen te behouden kan het brein informatie onthouden. In het leerproces van het brein staat zowel het aanmaken van neuronen, het maken van verbindingen en het onderhouden van deze verbindingen centraal [5]. Een neuron is de belangrijkste cel van het zenuwstelsel. Iedere neuron is een eigen microprocessor die signalen ontvangt en combineert vanuit verschillende andere neuronen. De communicatie tussen verschillende neuronen gaat via elektrische signalen [25]. De elektrische signalen zijn korte impulsen, ook wel spikes genoemd, in de spanning van de celmembraan. De verbindingen tussen neuronen komen tot stand via synapsen die zich aan de dendrieten bevinden. Ieder neuron staat in verbinding met duizenden andere neuronen en ontvangt meerdere signalen die uiteindelijk het cellichaam bereiken. Al deze signalen worden bij elkaar opgeteld en als het signaal een bepaalde waarde overschrijdt, wordt een spanning afgegeven. Dit signaal wordt via een zenuwvezel, een axon, doorgegeven aan andere neuronen. Een grafische representatie van dit proces kan worden gevonden in Afbeelding 1 [15].



Afbeelding 1: Essentiële onderdelen van een zenuwcel.

De synapsen, zoals te zien in Afbeelding 1, zijn de punten waar twee neuronen informatie kunnen overdragen. In het cellichaam en de axon worden neurostransmitters geproduceerd die worden overgebracht naar het einde van iedere axon. Aan het einde van iedere axon bevindt zich het presynaptische neuron. Vanuit het presynaptische neuron worden neurotransmitters vrijgelaten die in de synaptische spleet terechtkomen. De receptoren in het postsynaptische neuron binden zich aan de neurotransmitters waardoor de lading van de cel verandert. Dit proces is te zien in Afbeelding 2 [17].



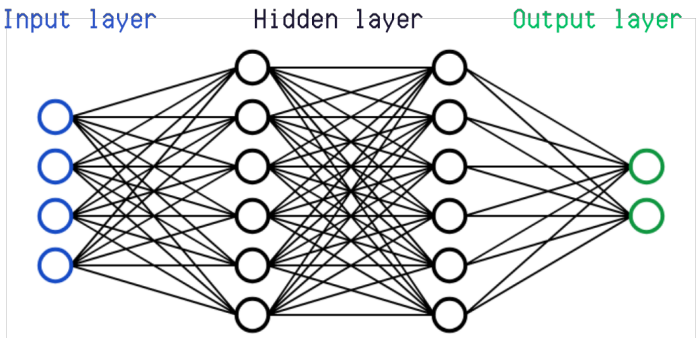
Afbeelding 2: Een synaps.

Om te bepalen of impulsen in een synaps gestuurd kunnen worden, kunnen signalen twee soorten effecten hebben. Er zijn signalen met een remmend effect en signalen die impulsgeneratie stimuleren. De onderscheidende verwerkingscapaciteit van iedere neuron hangt af van het type neuron en de sterkte van de synaptische verbindingen met andere neuronen.

Al deze miljarden zenuwcellen moeten alle signalen verwerken. Om dit allemaal in het brein te laten plaatsvinden, zijn deze verwerkingsprocessen optimaal. Neurale netwerken zijn geïnspireerd op dit optimale gebruik van de capaciteit van het brein. Deze netwerken zijn gesimplificeerde modellen van de netwerken van neuronen die ook voorkomen in de hersenen [15].

2.2 Neurale netwerken

De analogie van een neuron in een kunstmatig neuraal netwerk is een *node*. De dendrieten zijn de *inputs*. De axon wordt gerepresenteerd door de *output*. De sterkte van de synaptische verbindingen tussen neuronen is gegeven bij de *weights*. Omdat iedere connectie een eigen *weight* heeft, worden de *weights* van de verschillende connecties beïnvloed door de *weights* van alle *input* signalen. Dit leidt tot een sommatie, die ook wel de *weighted sum* wordt genoemd. Het resultaat is een intern activiteitsniveau voor de *node*. De *input data* worden vervolgens gewijzigd door middel van een overdrachtsfunctie. Deze overdrachtsfunctie kan ofwel van het drempeltype zijn, wat betekent dat informatie alleen wordt doorgegeven als het gecombineerde activiteitsniveau een bepaalde drempel bereikt, of het kan een continue functie zijn van de samengestelde *input data*. Een kunstmatig neuraal netwerk bestaat uit verschillende *layers* met *nodes* en de connecties tussen deze *layers*. Een grafische representatie van een kunstmatig neuraal netwerk is te vinden in Afbeelding 3.



Afbeelding 3: Kunstmatig neuraal netwerk.

Twee *layers* zijn verbonden met de buitenwereld. De *input layer* is de laag waar alle data aan het netwerk wordt gepresenteerd. De reactie van het netwerk op de *input layer* is de *output layer*. De *layers* ertussen zijn niet verbonden met de buitenwereld en worden ook wel de *hidden layers* genoemd [25]. De verbindingen tussen dendrieten, neuronen en axonen kunnen direct vergeleken worden met de *inputs*, *nodes* en *outputs* in een neuraal netwerk. Op deze manier beschrijft een kunstmatig neuraal netwerk een efficiënt netwerk geïnspireerd op de hersenen.

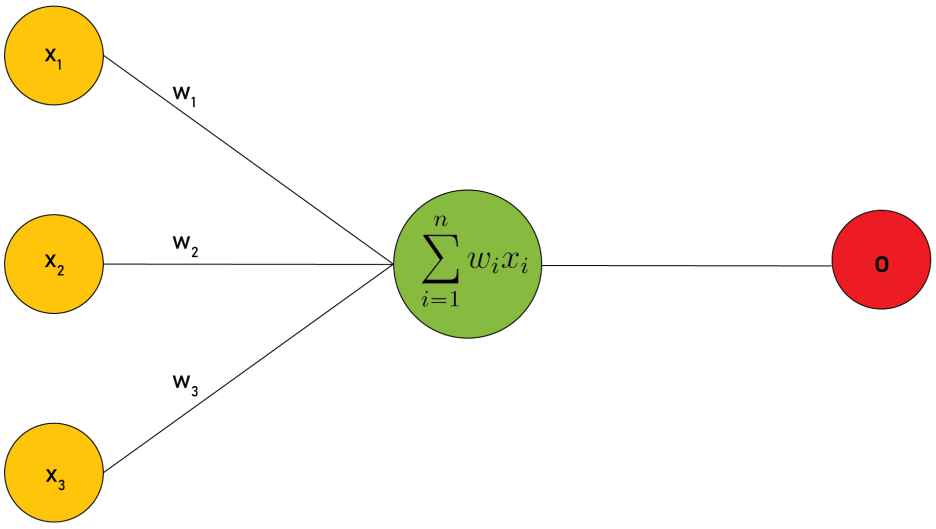
Het volgende hoofdstuk zal verder ingaan op de manier waarop neurale netwerken zijn opgebouwd vanuit wiskundig perspectief. Daarnaast zullen de verschillen tussen de neurale netwerken uitgelicht worden.

3 Neurale netwerken

Binnen neurale netwerken wordt gekeken naar artificiële neuronen. Een artificieel neuron kan zich in twee stadia bevinden. In de trainingsfase leert het neuron om specifieke *inputs* of *input*-patronen te verwerken. In operatiemodus geeft het neuron een *output* wanneer een bekend *input* patroon is gegeven. Als de *input* geen deel uitmaakt van de van te voren gedefinieerde *inputs*, dan besluiten de *fire* regels tezamen of er wel of niet een *trigger* gestuurd moet worden. Een elementair model van een neuron kan worden gesimuleerd door een computer [4].

3.1 Artificiele neuronen

Een kunstmatig neuron is een systeem met meerdere *inputs* en één *output*. De *inputs* worden gegeven door ruwe data en zijn genoteerd bij x_i voor $i = 1, \ldots, n$. Bij iedere *input* hoort een bepaalde *weight* gegeven door $w_1, w_2, \ldots, w_n$. Deze *weights* transformeren de *input* data. Wanneer alle *weights* en *inputs* van een netwerk samen genomen worden ontstaat er een sommatie gegeven bij $\sum_{i=1}^{n} w_i x_i$. De gegeven *output* is een *Threshold Logic Unit* (TLU). De activatie berekend door de sommatie wordt vergeleken met een bepaalde drempelwaarde. Als de activatie boven de drempelwaarde uitkomt, is de *output* **o** gelijk aan 1. Indien dit niet het geval is, dan zal de *output* **o** gelijk zijn aan 0 [15]. Op deze manier is iedere neuron een computationele *node* die een niet-lineaire functie representeert. Een grafische representatie van het artificiële neuron is te vinden in Afbeelding 4 [4].



Afbeelding 4: Een artificieel neuron.

Neurale netwerken hebben allerlei voordelen. Allereerst kunnen de netwerken henzelf aanpassen aan de omgeving tijdens het leren. Daarnaast heeft ieder getraind netwerk een erg goede generalisatiecapaciteit. Verder zijn de netwerken zelforganiserend. Ook hebben de netwerken de mogelijkheid om meerdere berekeningen parallel uit te voeren. Tot slot is het een robuust netwerk. Het netwerk is in staat om onnauwkeurige, *fuzzy* en probabilistische informatie te verwerken. Het is ook in staat om zichzelf te repareren [12].

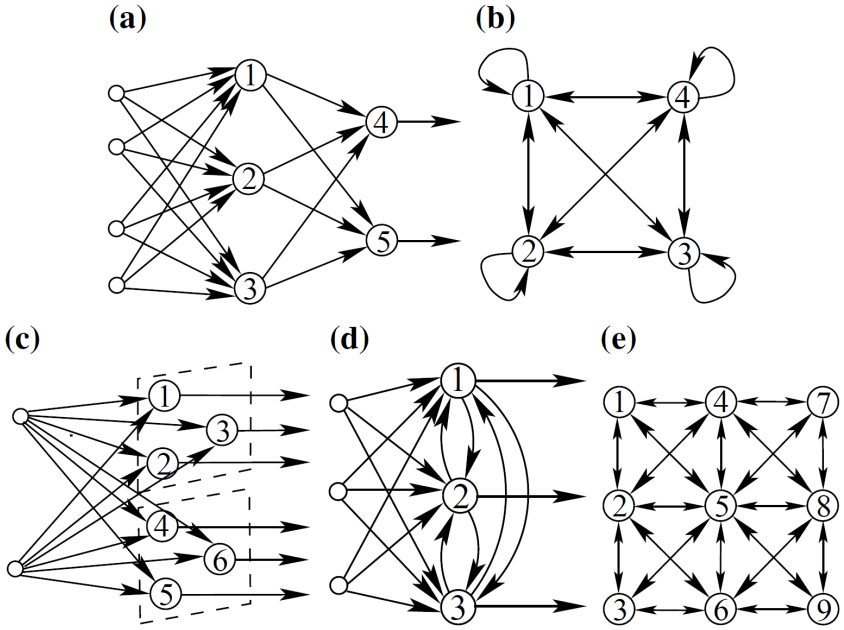
De toepassingen van neurale netwerken zijn erg divers. Met neurale netwerken kunnen functies benaderd worden. Dit wordt gebruikt om systemen te identificeren en te controleren, signalen te verwerken en patronen te herkennen en classificeren. Daarnaast kan er gegroepeerd worden. Objecten die soortgelijke eigenschappen hebben worden geclusterd.

Clusteren wordt vooral gedaan bij *neurofuzzy* systemen. Dit zijn systemen waarbij neurale netwerken samen met *fuzzy* logica worden gecombineerd. Bij *fuzzy* systemen is de uitkomst niet per sé juist of onjuist maar eerder deels juist of deels onjuist. Ook kunnen neurale netwerken gebruikt worden om problemen binnen de combinatoriek te optimaliseren. Ten slotte kan informatie samengevoegd worden [12]. Neurale netwerken zijn onder andere te vinden in de luchtvaart, de industrie, de transportsector, het bankwezen, elektronica en defensie [4].

Neurale netwerken verschillen in de manier waarop netwerken zijn opgebouwd, de karakteristieken van de *nodes* en de manier waarop geleerd wordt. De architectuur van het netwerk wordt gerepresenteerd bij de *connection-weights* matrix. Deze matrix is gegeven bij $\mathbf{W} = \left[w_{ij}\right]$, waarbij

$$w_{ij} = \begin{cases} 0, & \text{als er geen verbinding is tussen } \textit{node } i \text{ en } j. \\ 1, & \text{als er een verbinding is tussen } \textit{node } i \text{ en } j. \end{cases}$$

Wanneer er gekeken wordt naar de architectuur en de karakteristieken van de *nodes* kunnen neurale netwerken geclassificeerd worden als *Feedforward Neural Networks*, *Recurrent Neural Networks* en varianten hierop. Populaire typen netwerken zijn *Fully Connected Neural Layered Networks*, *Recurrent Networks*, *Lattice Networks*, *Layered Feedforward Networks* met laterale verbindingen en Cellular Networks. Deze vijf typen zijn te vinden in Afbeelding 5.



Afbeelding 5: (a) *Layered Feedforward Neural Network.* (b) *Recurrent Neural Network.* (c) *Two-dimensional Lattice Neural Network.* (d) *Layered Feedforward Neural Network* met laterale verbindingen. (e) *Cellular Neural Network.*

In een *Feedforward Neural Network* komen de verbindingen tussen neuronen in slechts één richting voor. In dit netwerk is er geen verbinding tussen de verschillende neuronen in een *layer* en is er geen terugkoppeling binnen één *layer*. In een *Fully Connected Neural Network* is iedere *node* in een *layer* verbonden met iedere *node* in de volgende *layer*. De *Multilayer Perceptron* en *Radial Basis Function Neural Network* zijn voorbeelden van *Fully Connected Neural Networks*. In een *Recurrent Neural Network*, bestaat er op zijn minst één terugkoppelingsverbinding. Het *Hopfield Model* en de *Boltzmann Machine* zijn voorbeelden van dit type netwerk. Een *Lattice Neural Network* bestaat uit één, twee of hogere dimensionale *array* van neuronen.

Iedere *array* heeft een bijbehorende set of *input nodes*. Het *Kohonen Neural Network* gebruikt een één of twee dimensionale lattice architectuur. Een *Layered Feedforward Neural Network* met laterale verbindingen heeft laterale verbindingen tussen neuronen in dezelfde *layer* van de *Layered Feedforward Neural Network* architectuur. *PCA Neural Networks* die *Hebbian* en *anti-Hebbian* regels om te leren gebruiken zijn voorbeelden. Een *Cellular Neural Network* bestaat uit neuronen die zich op eenzelfde afstand bevinden. Deze neuronen worden cellen genoemd. Deze cellen communiceren enkel met neuronen in de directe omgeving [12]. Diverse netwerken zullen worden besproken in de subsectie algoritmen.

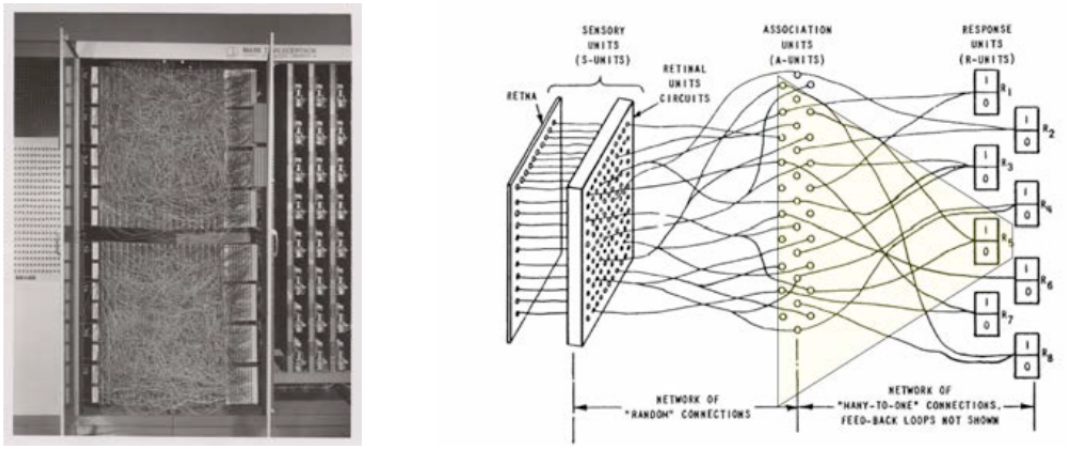
Neurale netwerken kunnen ook geclassificeerd worden aan de hand van de manier waarop het netwerk getraind wordt. Deze vier manieren zijn de *Fixed Weights* methode, *Unsupervised* training, *Supervised* training en *Reinforcement* training. In het geval van *Fixed Weights* zijn er geen waarden voor training en *weights*. Deze methode wordt bijvoorbeeld gebruikt om informatie te optimaliseren en inhoud te reduceren. Binnen *Unsupervised Learning* worden de *weights* alleen aangepast aan de hand van de gegeven *input*. Er is geen optimale *output* om de *weights* te corrigeren door de gewenste *output* en de daadwerkelijke *output* naast elkaar te leggen. De *weights* worden alleen aangepast aan de hand van de patrooninformatie van de *input*. Deze manier van leren wordt gebruikt binnen het classificeren en het vinden van gelijkenissen. Bij *Supervised Learning* gebeurt het tegenovergestelde. De *weights* worden aangepast nadat er feedback van de *output* error is gegeven. *Supervised* training wordt gedaan wanneer patroonherkenning moet worden gedaan. Tot slot wordt bij *Reinforcement Learning* de kwaliteit van het systeem stap voor stap verbeterd. Er zijn vaste manieren om te trainen maar de manier van trainen wordt aangepast aan de hand van de *output*. Deze methode bevindt zich tussen *Supervised* en *Unsupervised* training [10]. Zoals te zien is in Afbeelding 5 zijn er diverse typen neurale netwerken. De meest bekende netwerken zullen worden uitgelegd.

3.2 Algoritmen

In deze subsectie zullen drie verschillende soorten algoritmen besproken worden. Als eerste de *Feedforward* algoritmen, daarna de *Recurrent* algoritmen en tot slot de combinaties van deze twee algoritmen.

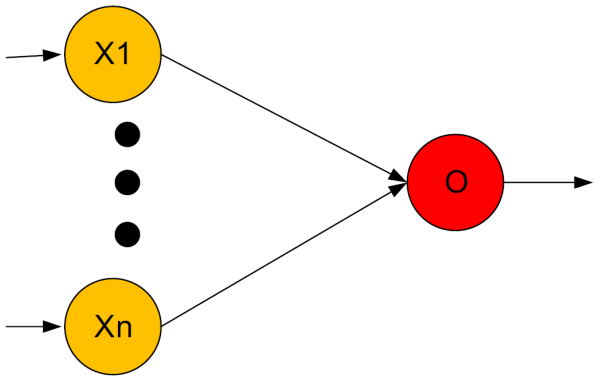
3.2.1 Feedforward Neural Networks

Het eerste artificiële neurale netwerk werd in 1958 al beschreven in een artikel door Rosenblatt. De perceptron was het eerste, zeer succesvolle *Machine Learning* concept. Naast de algoritmische ontdekking was Rosenblatt destijds in staat om ook de *Perceptron* te realiseren in hardware. Deze zogenoemde *Mark I Perceptron* was gerealiseerd in het Cornell Aeronautical Labratory. In Afbeelding 6 is links de hardware opstelling te zien. Rechts is de schematische weergave van de MARK I architectuur te zien. Het deel van het schema wat zich in de lichtgele driehoek bevindt, is de perceptron [7].



Afbeelding 6: De Mark I Perceptron.

Om een *Perceptron Neural Network* te snappen, wordt eerst naar haar minst gecompliceerde vorm gekeken. Het gaat hier over de *Single Layer Perceptron*. De opbouw van deze *Perceptron* is te zien in Afbeelding 7 [10].



Afbeelding 7: Een singe layer perceptron.

De *inputs* gegeven door x_i voor $i = 1, \ldots, n$ worden direct gecombineerd tot de *output* $\mathbf{o}$. De *input* van het neuron kan op de volgende manier berekend worden:

$$\begin{aligned} \mathbf{o} &= \phi(\text{net}), \text{ waarbij} \\ \text{net} &= \sum_{i=1}^{n} w_i x_i - \theta \\ &= \mathbf{w}^T \mathbf{x} - \theta, \end{aligned}$$

waarbij w_i en x_i respectievelijk the *input* en *weight* is voor *input* i, θ is de *threshold* en ϕ is de activatiefunctie. Voorbeelden van activatiefuncties zijn de Hard-Limiter Threshold Function, gegeven bij

$$\phi(x) = \begin{cases} 1, & x \geq 0, \\ -1, & x < 0, \end{cases}$$

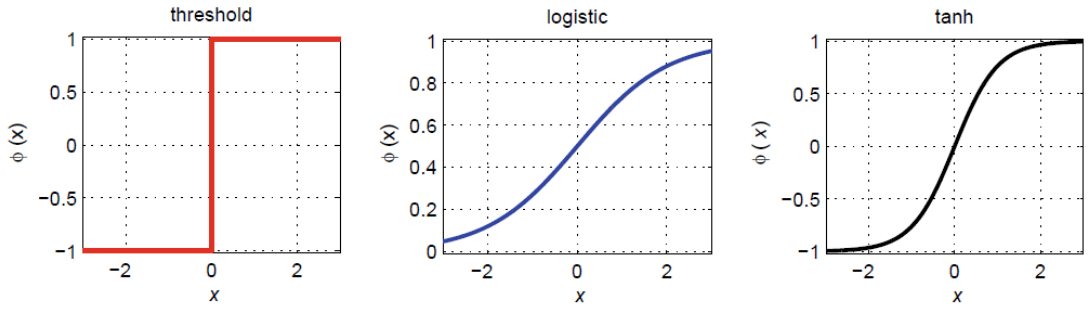
de *Logistic Function*

$$\phi(x) = \frac{1}{1 + e^{-\beta x}},$$

en tot slot de *Hyperbolic Tangent Function*

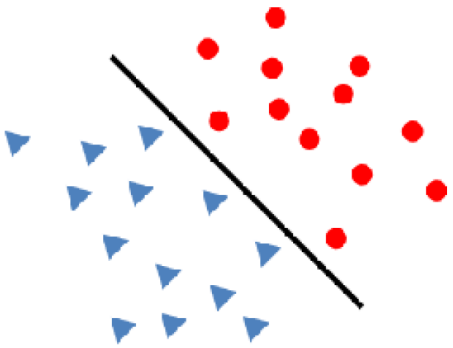
$$\phi(x) = \tanh(\beta x).$$

De grafieken van deze drie functies is ook te zien in Afbeelding 8 [12].



Afbeelding 8: Drie verschillende activatiefuncties.

Een *Perceptron* kan alleen leren van *input* die deelbaar is. Een *Perceptron* kan een lineaire functie leren die de data in twee groepen verdeelt. Deze functie wordt ook wel een *hyperplane* genoemd. Deze manier van leren is ook te zien in Afbeelding 9. Op deze manier kan de *Perceptron* bijvoorbeeld leren classificeren [10].

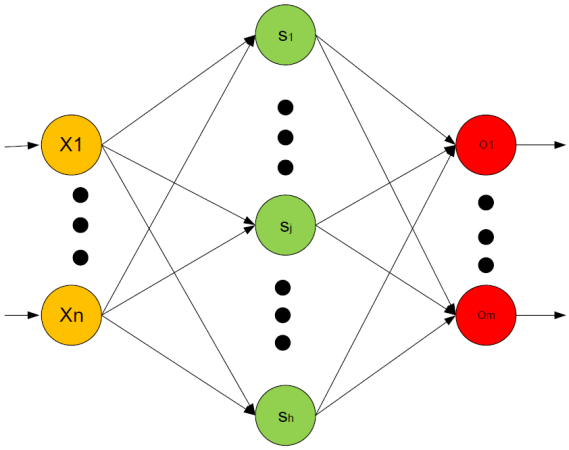


Afbeelding 9: *Linearly Separable Data.*

In Afbeelding 9 is een *Decision Boundary* te zien. Aan de linkerkant van deze *boundary* zijn de blauwe punten te zien, aan de rechterkant zijn de rode punten te zien. Deze *hyperplane* kan beschreven worden met de vergelijking

$$\mathbf{w}^T\mathbf{x} - \theta = 0.$$

Een nadeel van de *Single Layer Perceptron* is het feit dat het niet in staat is om nonlineaire problemen op te lossen. Voorbeelden van nonlineaire problemen zijn cirkels en spiralen. Een oplossing voor de nonlineairiteit kan gevonden worden als meerdere lagen worden toegevoegd. Dit leidt tot de *Multilayer Perceptron Neural Networks*, afgekort als *MLP Neural Network*. Een voorbeeld van een *MLP Neural Network* bestaande uit drie lagen is te zien in Afbeelding 10. In dit geval is n wederom het aantal *inputs*, h het aantal *hidden nodes* en m is de totale hoeveelheid *output nodes* [10].



Afbeelding 10: Een MLP neuraal netwerk met drie lagen.

In iedere iteratie wordt de *output* van de *hidden nodes* berekend door de volgende formule:

$$f(s_j) = \frac{1}{1 + \exp(-s_j)}. \tag{1}$$

Hierbij loopt j van 1 tot h en is de functie s_j gerepresenteerd door de volgende sommatie:

$$s_j = \sum_{i=1}^{n} w_{ij} \cdot x_i - \theta_j. \tag{2}$$

In deze vergelijking is w_{ij} wederom de *weight* tussen *input node* i en *node* j in de *hidden layer*. De *threshold* van *node* j in de *hidden layer* is gegeven door θ_j. Nadat de *output* van de *hidden nodes* is berekend, kan de uiteindelijke *output* berekend worden door Vergelijkingen (1) en (2) te combineren. Om de uiteindelijke *outputs* te berekenen kan de volgende formule gebruikt worden:

$$o_k = \sum_{j=1}^{h} w_{kj} \cdot f(s_j) - \theta_k. \tag{3}$$

Hier is w_{kj} wederom de *weight* maar in dit geval tussen *hidden node* j en de *output node* k. De error voor *output node* k is

$$E_k^{MLP} = \sum_{i=1}^{m} \left(o_i^k - d_i^k\right)^2. \tag{4}$$

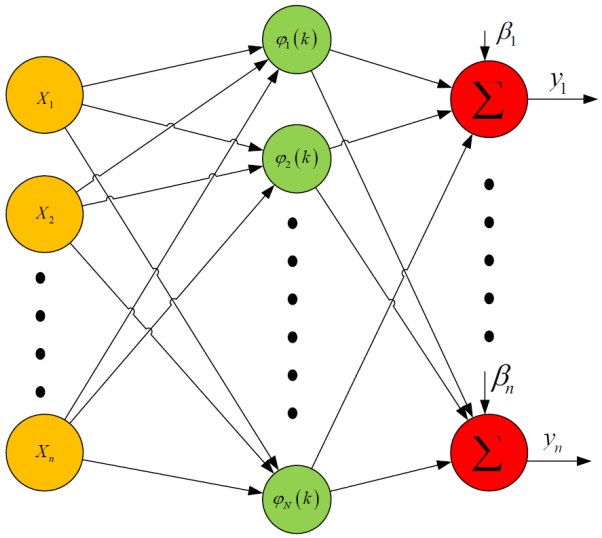
In dit geval is d_i^k de verwachte *output* [10]. Een soortgelijk *Feedforward Neural Network* is de *Multilayer Perceptron* is de *Radial Basis Function Neural Network*. Dit wordt ook wel afgekort als *RBF Neural Network*. Dit netwerk bestaat uit dezelfde drie lagen als de *MLP Neural Network* maar in dit geval wordt de *output* of de *input layer* aangepast door de afstand tussen de *inputs* en de *centers* van de *hidden layer* te berekenen. Er wordt aangenomen dat iedere neuron in de *hidden layer* een *center* heeft, in deze *center* kan informatie verwerkt worden. De *outputs* van de *hidden layer* worden berekend door de outputs van de *input layer* ende bijbehordende *weight* te vermenigvuldigen. Dit is dezelfde sommatie als eerder genoemd in Afbeelding 4. De *output* van de *RBF Neural Network* is

$$\hat{y}_j = \sum_{i=1}^{I} w_{ij} \phi\left(||x - c_i||\right) + \beta_j, \tag{5}$$

waarbij I het totale aantal *hidden* neurons is, w_{ij} wederom de *weight* representeert en β_j is de *bias* van neuron j in de *output layer*. Één van de activatie functies voor een *RBF Neural Network* is de *Gaussian Basis Function* en deze functie wordt geschreven als

$$\varphi(r) = \exp(\left(-\alpha_i||x - c_i||^2\right), \tag{6}$$

waar a_i de *variance* parameter is en c_i is de *center vector* voor neuron i. Een *RBF Neural Network* met één *hidden layer* is te zien in Afbeelding 11 [10].

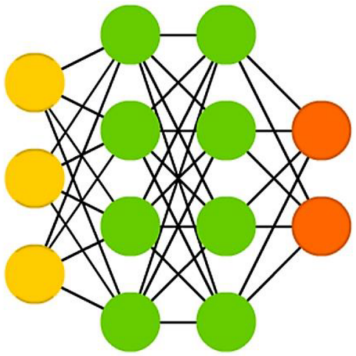


Afbeelding 11: Een *Radial Basis Function Neuraal Netwerk* met drie lagen.

De error is in het geval van een *RBF Neural Network* gelijk aan

$$E^{RBF}(w, a, c, \beta) = \sum_{i=1}^{I}(\hat{y}_j - y_j)^2, \tag{7}$$

waarbij $\hat{y}_j$ de berekende *output* representeert en y_j de gewenste *output*. Het doel van het trainen van *RBF Neural Networks* is het minimaliseren van de *Root Mean Squared Error*, afgekort als *RMSE*, ofwel het minimaliseren van de error in vergelijking (7). Een *Feedforward Neural Network* zoals het *RBF Neural Network* kan ook meerdere hidden layers hebben. Indien dit het geval is, heet dit een *Deep Feedforward Neural Network*. Dit wordt ook wel afgekort als *DFF Neural Network*. De opbouw van dit netwerk is te zien in Afbeelding 12.

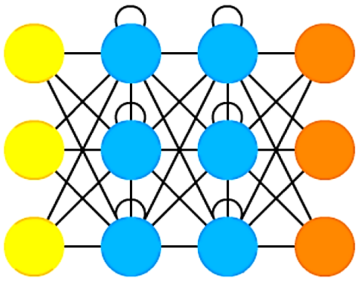


Afbeelding 12: Een *Deep Feedforward Neural Network*.

Het voordeel van dit netwerk is dat het veel betere resultaten geeft dan neurale netwerken met slechts één *hidden layer*. Om deze reden vormen deze netwerken dan ook de basis van moderne *Machine Learning* systemen. Het nadeel aan deze netwerken is dat er veel rekenkracht en dus rekentijd voor nodig is.

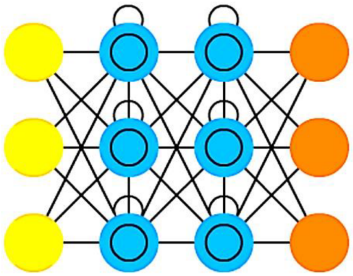
3.2.2 Recurrent Neural Networks

Bij een *Feedforward Network* komen de verbindingen slechts in één richting voor en er is geen verbindingen tussen neuronen in een *layer* of een terugkoppeling voor het neuron zelf. Dit is anders in *Recurrent Neural Networks*. Binnen dit netwerk ontvangt iedere *hidden recurrent cell* zijn eigen *input* met een bepaalde vertraging. Op deze manier hebben beslissingen uit het verleden invloed op de huidige beslissing. Dit type netwerk wordt vooral gebruikt wanneer de context belangrijk wordt. Het netwerk is te zien in Afbeelding 13.



Afbeelding 13: Een *Recurrent Neural Network*.

Waar reguliere *Recurrent Neural Networks* in staat zijn om een klein deel van de beslissingen uit het verleden in gedachten te houden, zijn *Long Short-Term Memory Neural Networks*, afgekort als *LSTM Neural Networks*, in staat om beslissingen die lang geleden hebben plaatsgevonden in gedachten te houden. Iedere *memory cell* bestaat uit een paar *gates*, die terugkerend zijn en in de gaten houden hoe informatie wordt herinnerd envergeten. De *input gate* besluit hoeveel informatie uit de laatste *sample* in het geheugen blijft en de *output gate* reguleert de hoeveelheid data dat naar de volgende *layer* gaat. Een voorbeeld van dit netwerk is te vinden in Afbeelding 14.

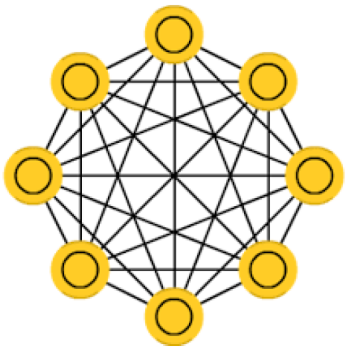


Afbeelding 14: Een *Long Short-Term Memory Neural Network*.

3.2.3 Combinatie van Feedforward en Recurrent Neural Networks

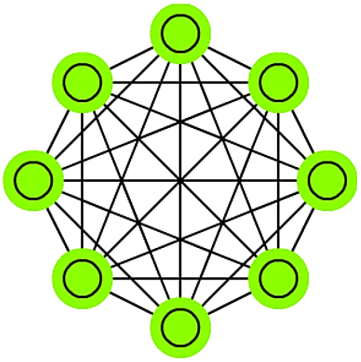
Twee voorbeelden van combinaties van *Feedforward* en Recurrent Neural Networks zijn het *Hopfield Neural Network* en de *Markov Chains Networks*. Een *Hopfield Neural Network* heeft een eigen architectuur. De *input* neuronen zijn hier ook de *output* neuronen. Er zijn geen *weights* gespecificeerd maar er is een detectiealgoritme waarin *inputs* herhaald en aangepast worden op een bepaalde manier. In dit geval ontvangt één neuron *inputs* van andere neuronen.

Met deze *inputs* wordt deze ene neuron veranderd en blijven de andere neuronen hetzelfde. Deze architectuur is ook duidelijk te zien in Afbeelding 15 [10].



Afbeelding 15: Een *Hopfield Neural Network*.

Het *Hopfield Neural Network* was het eerste *Neural Network* dat gebruikt werd om *The Traveling Salesman Problem* op te lossen. Dit is een van de meest bekende optimalisatie problemen. In dit geval is er een afstand $d_{ab} = d_{ba}$ gegeven. Hierbij moet een weg gevonden om van a naar b (of andersom) te lopen waarbij de afstand zo klein als mogelijk moet zijn [14]. Het *Markov Chains Network* heeft een soortgelijke structuur als een *Hopfield Neural Network* zoals te zien is in Afbeelding 16 [10].



Afbeelding 16: Een *Markov Chains Network*.

Als er een verdeling bestaat waarvoor geen directe kwantitatieve toegang mogelijk is, is een ideale benadering om *samples* te nemen uit de verdeling totdat er voldoende *samples* zijn verkregen. Het nemen van *random samples* uit een gedeeltelijk onbekende verdeling $\phi(x)$ staat bekend als de *Markov Chain Sampling*. Een *sampling process* is *Markov* als de eerst volgende *state-space* alleen afhangt van de vorige *state-space*. Dit kan beschreven worden bij het volgende iteratieve proces:

$$\phi(x_{t+n\tau}) = k_t \pi_t.$$

waarbij k de *transition kernel* van het *Markov process* is en $\phi(x_{i+1})$ de gewenste verdeling. Een *stochastic sampled path* van een irreduceerbare en aperiodieke *Markov Chain* heeft van nature een stationaire verdeling op tijdstip $t \to \infty$. Daarom vraagt het vinden van de stationaire verdeling $\pi(x)$ van een *Markov Chain* een *transition kernel* k van $(n\tau)$-tijd, zodat;

$$\phi(x_{i+1}) = k\pi(x_i).$$

Een *Markov Chain* met een stationaire verdeling $\pi(x)$ staat ook bekend als tijdsomkeerbaar als de bijbehorende *transition kernel* k voldoet aan een voorwaarde die *detailed balance* wordt

genoemd. Dit wordt beschreven door

$$\pi(x)k(x,y) = \pi(y)k(y,x).$$

Deze notie geldt ook de andere kant op. Een *Markov Chain* is tijdsomkeerbaar met een *kernel* die voldoet aan de *detailed balance* hierboven moet een stationaire verdeling hebben [18].

Met Feedforward Neural Networks, Recurrent Neural Networks en combinaties van deze beide wordt een goede basis voor allerlei neurale netwerken die door bedrijven worden gebruikt beschreven.

4 Marktonderzoek

Allereerst wordt de interesse van de Rijksinspectie Digitale Infrastructuur, afgekort als RDI, in de richting van neurale netwerken uitgelegd. Daarna wordt een marktonderzoek dat is uitgevoerd tijdens de stage voorgelegd.

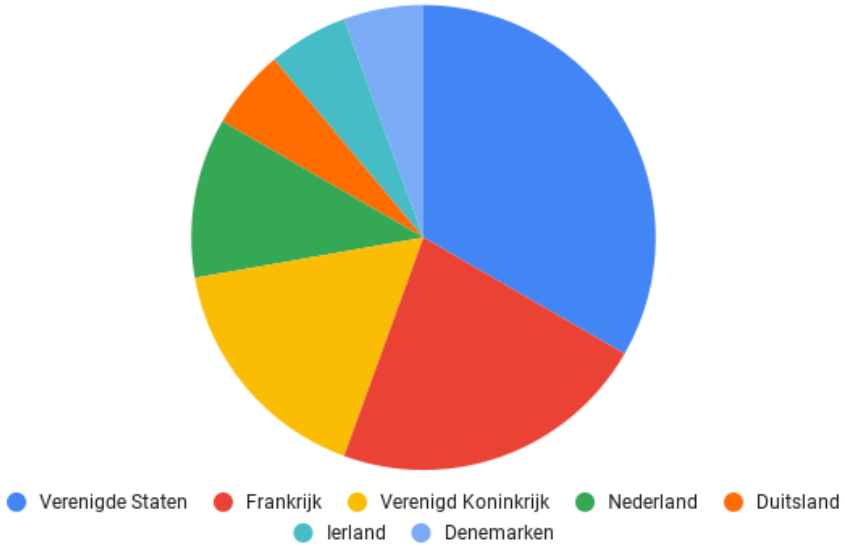
4.1 Missie

De Rijksinspectie Digitale Infrastructuur wenst een toezichthouder te worden op het gebied van artificiële intelligentie. Gezien de RDI momenteel ook al toezicht houdt op infrastructuur en digitale weerbaarheid is er een reeële kans dat de RDI deze toezichthouder wordt. Op 21 april 2021 is de Artificial Intelligence Act, de AI Act, voorgesteld door de Europese Unie [8]. Het gebruik van AI in de Europese Unie zal gereguleerd worden door de AI Act. Het doel hiervan is het beschermen van burgers door middel van een begrijpelijke wetgeving. Op het moment van schrijven wordt er nog druk onderhandeld over hoe de wetgeving er uit moet komen te zien. Het doel is om in 2026 toezicht te houden op artificiële intelligentie [21]. Om haar voor te bereiden op het mogelijke toezichthouderschap, wil de RDI kennis vergaren omtrent het gebruik van neural netwerken binnen bedrijven.

4.2 Bedrijven

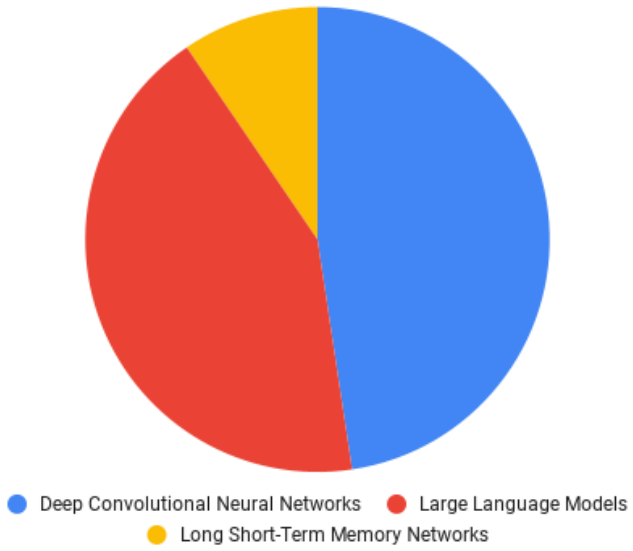
Om een beter beeld te krijgen van het gebruik van neurale netwerken bij bedrijven, zijn achttien bedrijven die artificiële intelligentie gebruiken ondervraagd. Allereerst is aan hen gevraagd wat het gebied van expertise is betreffende neurale netwerken en hieropvolgend is gevraagd welk type neurale netwerken zij het meest gebruiken, danwel het meest voorbij zien komen. De ondervraagde bedrijven waren werkzaam in de consultancy, bouwden aan een kennisplatform of genereerden zelf toepasingen op het gebied van artificiële intelligentie. De bedrijven werkten met neurale netwerken op het gebied van beelden, generatieve artificiële intelligentie en de zogenoemde *Large Language Models*. De namen van de bedrijven zijn bij de auteur bekend.

Om een zo goed mogelijk beeld te krijgen van de huidige markt, zijn bedrijven uit verschillende landen ondervraagd. Het gaat hier om Amerikaanse en Europese bedrijven. De afkomst van deze bedrijven zijn te vinden in Afbeelding 17.



Afbeelding 17: De afkomst van de ondervraagde bedrijven.

De drie meest genoemde neurale netwerken zijn *Deep Convolutional Neural Networks*, *Large Language Models* en *Long Short-Term Memory Neural Networks*. Wanneer bedrijven werken met afbeeldingen om bijvoorbeeld iets te herkennen van de afbeelding of om een afbeelding om te zetten naar tekst worden veelal *Deep Convolutional Neural Networks* gebruikt. Dit is dan ook het meest gebruikte neurale netwerk uit de groep respondenten. Veel gebruikte families uit de *Deep Convolutional Neural Networks* zijn *YOLO* en *ResNet* [19]. Naast de afbeeldingen wordt er ook veel artificiële gegenereerd. Dit heet ook wel *generative AI*. De ondervraagde bedrijven die *generative AI* gebruikten, werkten met *Large Language Models*. Een bekend voorbeeld is ChatGPT van OpenAI [3]. De ondervraagde bedrijven ontwikkelden zelf geen *Large Language Models*. Zij maakten gebruik van reeds getrainde *Large Language Models* van andere bedrijven. Als derde worden *Long Short-Term Memory Neural Networks* gebruikt. De *LSTM* is een subfamilie van de *Recurrent Neural Networks*. De *LSTM Neural Networks* zijn voornamelijk goed in het verwerken van lange reeksen data in plaats van individuele data punten. Op deze manier zijn *LSTM Neural Networks* bijvoorbeeld zeer geschikt voor het herkennen van spraak [28]. De verdeling van de drie meest genoemde neurale netwerken is ook te zien in Afbeelding 18.



Afbeelding 18: De drie meest genoemde neurale netwerken.

Naast de drie grootste pijlers werden ook andere belangrijke aspecten aangedragen door de bedrijven. Allereerst gaven een aantal bedrijven aan te werken met *TinyML*. Dit staat voor *Tiny Machine Learning*. Dit type *Machine Learning* wordt gebruikt om ook modellen op kleinere, minder krachtige apparaten te kunnen draaien. Daarnaast wordt dit ook gebruikt om de energieconsumptie te verlagen. Binnen het werkgebied van *TinyML* wordt zowel gekeken naar de hardware, algoritme en software [16]. Daarnaast werden *Multimodels* aangehaald. Soms zijn problemen zo complex dat ze niet met één model op te lossen zijn. Op dat moment worden er meerdere modellen gecombineerd. Dit is het op *Machine Learning* gebaseerde *Multimodel Computing*. Binnen deze manier van rekenen kunnen meerdere neurale netwerken worden ingezet om zo één groot model te genereren die moeilijke problemen op te lossen. Dit wordt bijvoorbeeld veel in de medische wereld gebruikt om afwijkingen te kunnen detecteren [2].

5 Artificiële Intelligentie binnen de RDI

Naast dat de Rijksinspectie Digitale Infrastructuur graag een toezichthouder wil worden omtrent het onderwerp AI, heeft zij zelf ook een taak om veiligheid te garanderen op het gebied van de elektronische identiteit. Met een toenemend aantal aanvallen op de elektronische identiteit is dit een belangrijk punt op de agenda van de RDI [26].

5.1 Vertrouwensdiensten

De Rijksinspectie Digitale Infrastructuur houdt toezicht op vertrouwensdiensten die de eIDAS verordening en Telecomwet handhaven. Een vertrouwensdienst is een basisdienst voor bijvoorbeeld elektronische handtekening, elektronische zegels en tijdstempels. Hierbij staat de koppeling tussen de fysieke identiteit en de elektronische identiteit centraal. Het doel is om iemand te kunnen identificeren zonder een fysieke afspraak te hoeven maken. Dit wordt gedaan met de zogenoemde identificatiesystemen. Deze vertrouwensdiensten kunnen in twee verschillende niveaus vallen. Niveau 1 is het hoogste niveau. Binnen niveau 1 vallen de gekwalificeerde vertrouwensdiensten. De acties van deze vertrouwensdiensten hebben rechtsgevolgen in heel Europa. Om deze reden staan deze vertrouwensdiensten onder permanent toezicht bij de RDI. Onder niveau 2 vallen de ongekwalificeerde vertrouwensdiensten. De RDI gaat toezicht houden op het moment dat er incidentmeldingen zijn of als de RDI berichten over deze dienst krijgt.

Naast het toezicht houden op deze vertrouwensdiensten, houdt de RDI ook toezicht op de eID aanbieders die de eIDAS verordening en Wet Digitale Overheid handhaven. De eID aanbieders bieden elektronische identiteiten aan. De afkorting eIDAS staat voor Electronic Identities and Trust Services. Met deze verordening hebben alle Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een belangrijk onderdeel van deze verordening is het gebruik van inlogmiddelen die Europees erkend zijn [22].

Het op afstand bevestigen van de identiteit van een persoon wordt in diverse sectoren zoals vervoer, gezondheidszorg en het bankwezen gebruikt. In de tijden van de COVID-19 pandemie is het gebruik van identificatie op afstand sterk toegenomen. Gedurende het proces van identificatie worden drie stappen gehanteerd. Allereerst wordt het identiteitsdocument geverifieerd. Er kan een optische verificatie plaatsvinden waarbij onder andere gekeken wordt naar de echtheidskenmerken van het paspoort. Daarnaast kan ook de NFC chip gebruikt worden. De afkorting NFC staat voor Near Field Communication. Deze chip zit in de telefoon die op een afstand van maximaal tien centimeter de informatie van het identiteitsdocument kan uitlezen [23]. Nadat het identiteitsdocument is geverifieerd, moet er gekeken worden of er een echt persoon deelneemt aan het proces. Ten slotte moet er een vergelijking gemaakt worden tussen het identiteitsdocument en de persoon die deelneemt. Er wordt een kans berekend dat de persoon die deelneemt aan het proces overeenkomt met de persoon op het identiteitsdocument.

De normen om toezicht te houden zijn niet wettelijk verplicht. Deze normen zijn zogenaamde open normen. In deze normen staat bijvoorbeeld nergens een vastgestelde waarde voor accuraatheid. Ondanks dat de normen niet wettelijk verplicht zijn, is het wel wettelijk verplicht om een audit te doen en de auditors gebruiken de ETSI normen. De eIDAS verordening is ook beschreven in ETSI normen in ETSITS119461. Momenteel wordt er per zaak toezicht gehouden, er is niet één uniforme, specifieke wetgeving. Deze manier van toezicht houden geeft diverse uitdagingen.

Allereerst moet er een bepaalde meetzekerheid gegeven worden. Echter, het proces bestaat uit drie stappen: De verificatie van het identiteitsdocument, de echtheid van de persoon en ten slotte de vergelijking tussen deze twee. Van al deze drie stappen kan een bepaalde meetzekerheid gemeten worden. De vraag die dan open staat is; hoe worden deze drie waarden daarna gecombineerd tot één waarde? Daarnaast is de vraag hoe betrouwbaar de bron is. Er is natuurlijk weinig testdata beschikbaar als het om identiteitsdocumenten gaat, mensen stellen die niet ter beschikking uit angst voor identiteitsfraude. Naast de meetzekerheid zit de uitdaging ook in de toeleveringsketen. Allereerst ligt de vraag er of we hier spreken over een product of over een dienst. Daarnaast is er de vraag hoe de systemen geïntegreerd moeten worden. Tot slot houdt de RDI toezicht op de vertrouwensdiensten binnen de Europese Unie. In hoeverre kan de RDI ook toezicht houden op leveranciers van buiten de Europese Unie? Behalve de toeleveringsketen en de meetzekerheid liggen er ook uitdagingen in de cyberveiligheid. Allereerst moet de betrouwbaarheid van het systeem gegarandeerd kunnen worden. De data moet beveiligd zijn, er zal een soort van eindcontrole moeten zijn en pentests zullen moeten worden uitgevoerd. Een pentest is een afkorting voor een penetratietest. Dit is een gesimuleerde cyberaanval op één van de te testen systemen [6]. Naast deze drie uitdagingen speelt artificiële intelligentie ook een grote rol in het toezicht houden.

5.2 Artificiële Intelligentie

Artificiële intelligentie kan gebruikt worden om identiteitsfraude te plegen. Er worden aanvallen gedaan op de systemen om zo binnen te komen bij een bepaalde dienst met een andere identiteit. De meeste aanvallen vinden plaats in de eerste stap; de identiteitsdocumentverificatie. De identificatie met de NFC chip is veilig. Deze data is beveiligd met een persoonlijke versleutelcode. Daarentegen wordt de optische verificatie veelal aangevallen. Hierbij worden de echtheidskenmerken bijvoorbeeld geprojecteerd op het identiteitsdocument om het echt te laten lijken. Daarnaast kan ook de foto van de persoon op het identiteitsdocument aangepast worden door er een laag overheen te leggen. Dit wordt gedaan met de tekstuele informatie op het identiteitsdocument. Wanneer er gecontroleerd moet worden of de persoon op de camera een echt persoon is, worden steeds geavanceerde aanvallen gedaan. Zo worden er bijvoorbeeld schermen geplaatst voor de camera waarop een deel van de film te zien is. Ook kan er gebruikgemaakt worden van een virtuele camera. In deze camera kan een *deep fake* afgespeeld worden. Een *deep fake* is een kunstmatig gegenereerde video waarbij bijvoorbeeld een gezicht van een bepaald persoon over het gezicht van een ander persoon geplakt kan worden. Op deze manier kan de aanvaller zich voordoen als de persoon van wie de aanvaller de identiteit wil stelen [1]. In de laatste stap, de biometrische vergelijking, zijn op dit moment geen aanvallen bekend.

Om de veiligheid van Nederland te garanderen is het belangrijk dat er meer kennis komt over de gevaren en kansen van artificiële intelligentie. Binnen de RDI is daarom ook het AI-programma gestart. Binnen dit programma staat zowel het leren begrijpen van AI als het ontwikkelen van tools centraal. Bij het ontwikkelen van tools kan dit gedaan worden om andere afdelingen binnen de RDI te helpen. Zo worden er diverse tools ontwikkeld zodat het werk van de inspecteurs vergemakkelijkt wordt. Naast het vergaren van algemene kennis en het ontwikkelen van tools wordt er ook gefocust op het veilig houden van de elektronische identiteit. Om de veiligheid te kunnen borgen wil de RDI graag dat er wetten komen omtrent dit onderwerp. Deze wetgeving moet hetzelfde zijn voor de gehele Europese Unie. Naast het vaststellen van wetten, moeten ook de standaarden worden uitgebreid. Zo moeten er normen komen om de prestaties van artificiële intelligentie bij te houden. Wanneer wetten en standaarden worden gevormd, zullen deze ook gehandhaafd moeten worden. Daarom moet het testproces geharmoniseerd worden. Één van de wensen van de RDI is een eigen testlab om bijvoorbeeld *deep fakes* te kunnen detecteren. Op deze manier kan er, onafhankelijk van derde partijen, getest worden.

Tot slot is dit een onderwerp dat voortdurend verandert. De RDI wil graag een volwassen systeem ontwikkelen door statistieken bij te houden en ervaringen en incidenten te delen [13].

5.3 AI-Testlab

Een van de wensen van de RDI is naast het hebben van een IoT Testlab, ook een eigen testlab voor AI te ontwikkelen. Binnen het IoT-Testlab worden op dit moment testen gedaan met digitale apparatuur. Hierbij wordt bijvoorbeeld gekeken of een apparaat geen andere apparaten verstoort. Veel slimme, digitale apparaten werken namelijk op dezelfde frequentie. Dit lab bevindt zich nu in de vestiging van de RDI in Amersfoort. In het AI-Testlab wordt de werking van algoritmes onder de loep genomen en wordt bekeken hoe de veiligheidsniveaus kunnen worden ingebouwd [26]. Algemene testen die kunnen worden uitgevoerd in het lab zijn bijvoorbeeld het herkennen van snijrandjes. Wanneer een deepfake gegenereerd wordt, wordt het hoofd van de ene persoon op het hoofd van het andere persoon geplakt. Dit gaat nog niet altijd foutloos, dan is er een randje van het masker te zien. Ook bij het plakken van echtheidskenmerken op een identiteitsdocument kunnen soms snijrandjes verschijnen. Daarnaast kan er gekeken worden of er menselijk gedrag wordt vertoond. Als er een *deep fake* gegenereerd wordt, wil een hoofd nog weleens bewegen op een manier die fysiek onmogelijk is voor de mens. Naast deze algemene tests kunnen er ook meer geavanceerde tests ingezet worden. Zo kan er gekeken worden naar biologische signalen. Aan de hand van de hartslag verandert de roodheid van het gezicht van een persoon. Er kan gecontroleerd worden op deze roodheid om te controleren of het beeld een *deep fake* in plaats van een echt persoon is [9]. Een andere manier is het sturen van reeksen van verschillende kleuren licht die dan op een bepaalde manier teruggekaatst moeten worden. Omdat deze reeks tot op heden niet geraden is, kan deze technologie goed ingezet worden om *deep fakes* te detecteren [27].

Voor het detecteren van niet-menselijk gedrag en de snijrandjes zijn veel tools, ook open source, beschikbaar. Deze zouden makkelijk geïmplementeerd kunnen worden in het AI-Testlab. Het implementeren van meer geavanceerde methodieken zoals biologische signalen is een uitdagender proces hoewel dit niet onmogelijk is omdat er al veel over is geschreven.

6 Conclusie

Het menselijk brein leert door verbindingen te maken tussen verschillende zenuwcellen. Deze zenuwcellen worden aangemaakt en de verbindingen moeten worden onderhouden. Neurale netwerken zijn geïnspireerd op de werking van het menselijk brein. De zenuwcellen in ons brein zijn de *nodes* in een artificieel neuraal netwerk, de dendrieten zijn de *inputs* en de axonen de *outputs*.

Als er gekeken wordt naar de architectuur en karakteristieken van de neurale netwerken, kunnen deze geclassificeerd worden als *Feedforward Neural Networks*, *Recurrent Neural Networks* en de varianten hierop. Populaire typen neurale netwerken zijn *Fully Connected Neural Layered Networks, Recurrent Neural Networks, Lattice Neural Networks, Layered Feedforward Neural Networks* met laterale verbindingen en *Cellular Neural Network*.

Neurale netwerken zijn een onderdeel van machine learning. Machine learning is een onderdeel van artificiële intelligentie. Artificiële intelligentie is een onderwerp dat ook op de agenda van de RDI staat aangezien de RDI voor een veilig verbonden Nederland staat. Op 21 april 2021 is de AI Act voorgesteld door de EU en in 2026 moet er toezicht gehouden worden. De RDI wil ook graag een toezichthouder worden. Om dit te kunnen doen wilde de RDI graag een inventarisatie van het gebruik van neurale netwerken door bedrijven hebben. Er blijkt dat zowel *Long Short-Term Memory Networks, Deep Convolutional Neural Networks* en *Large Language Models* het meest gebruikt worden door de achttien ondervraagde bedrijven.

Momenteel houdt de RDI al toezicht op de vertrouwensdiensten die de eIDAS verordening en Telecomwet handhaven. De gevaren van artificiële intelligentie bij deze vertrouwensdiensten zit zowel in het vervalsen van het identiteitsdocument als het gebruiken van *deep fakes* in virtuele camera's. De RDI wil graag een AI-Testlab opzetten om onder andere *deep fakes* te kunnen herkennen maar ook om algoritmen die gebruikt worden binnen AI te kunnen bestuderen en de ingebouwde veiligheidsmaatregelen te kunnen controleren.

Om een goede toezichthouder te blijven is het belangrijk om voldoende kennis te hebben, daarom is het advies dan ook om te blijven investeren in kennis binnen artificiële intelligentie. Dit kan bijvoorbeeld op het gebied van wiskunde, op het gebied van hardware en ook op het gebied van dataverwerking. Door goed te communiceren over de expertises van medewerkers en te blijven samenwerken binnen de verschillende werkgroepen, zal de RDI een goede toezichthouder blijven, ook op het gebied van artificiële intelligentie en met name de meest gebruikte subgroep; de neurale netwerken.

Bronnenlijst

[1] Shruti Agarwal et al. "Detecting deep-fake videos from appearance and behavior". In: *2020 IEEE international workshop on information forensics and security (WIFS)*. IEEE. 2020, pp. 1–6.

[2] Fatemah H Alghamedy et al. "Machine Learning-Based Multimodel Computing for Medical Imaging for Classification and Detection of Alzheimer Disease". In: *Computational Intelligence and Neuroscience* 2022 (2022).

[3] Valentina Alto. *Modern Generative AI with ChatGPT and OpenAI models: leverage the capabilities of OpenAI's LLM for productivity and innovation with GPT3 and GPT4*. 2023.

[4] Dave Anderson and George McNeill. "Artificial neural networks technology". In: *Kaman Sciences Corporation* 258.6 (1992), pp. 1–83.

[5] Hasan Ayaz and Frederic Dehais. *Neuroergonomics: The brain at work and in everyday life*. Academic Press, 2018.

[6] Aileen G Bacudio et al. "An overview of penetration testing". In: *International Journal of Network Security & Its Applications* 3.6 (2011), p. 19.

[7] Michael Biehl. "The Shallow and the Deep". In: (2022).

[8] European parlement: Briefing. *Artificial Intelligence Act*. 2023.

[9] Umur Aybars Ciftci, Ilke Demir, and Lijun Yin. "Fakecatcher: Detection of synthetic portrait videos using biological signals". In: *IEEE transactions on pattern analysis and machine intelligence* (2020).

[10] Alexander Doug. *Neural Networks: History and Applications*. Nova, 2020.

[11] "Drie manieren waarop generative AI de telecomindustrie zal veranderen". In: (2023). URL: `https://www.winmagpro.nl/hoe-ai-en-machine-learning-de-toekomst-van-bedrijven-zullen-beinvloeden`.

[12] Ke-Lin Du and Madisetti NS Swamy. *Neural networks and statistical learning*. Springer Science & Business Media, 2013.

[13] Gerard Feitsma. *Remote Identity Proofing: Current situation and challenges in The Netherlands*. ENISA Workshop, 2023.

[14] Stephen I Gallant. *Neural network learning and expert systems*. MIT press, 1993.

[15] Kevin Gurney. *An introduction to neural networks*. CRC press, 2018.

[16] Gian Marco Iodice and Ronan Naughton. *TinyML Cookbook: Combine artificial intelligence and ultra-low-power embedded devices to make the world smarter*. Packt Publishing Ltd, 2022.

[17] Marcel Loeffen. *Synaps*. Brainmatters, 2022.

[18] Pierre Lorrentz. *Artificial neural systems: Principle and practice*. Bentham Science Publishers, 2015.

[19] Umberto Michelucci. *Advanced applied deep learning: convolutional neural networks and object detection*. Springer, 2019.

[20] "Missie, visie, kernwaarden". In: (2023). URL: `https://www.rdi.nl/over-ons/organisatie/missie`.

[21] European parlement: News. *EU AI Act: first regulation on artificial intelligence*. 2023.

[22] Digitale Overheid. *eIDAS*. 2023.

[23] Robert R Sabella. *NFC for Dummies*. John Wiley & Sons, 2016.

[24] Nassia Skoulikariti. “Hoe AI, IoT en 5G de economische groei aanjagen”. In: (2023). URL: https://tbmnet.nl/hoe-ai-iot-en-5g-de-economische-groei-aanjagen/.

[25] Ivan Stanimirović. *Deep Neural Networks and Applications*. Arcler Press, 2020.

[26] Diederik Toet. “RDI begint ai-lab om ontwikkelingen bij te benen”. In: *Computable* (2023).

[27] Zhiming Xia et al. “Towards DeepFake video forensics based on facial textural disparities in multi-color channels”. In: *Information Sciences* 607 (2022), pp. 654–669. URL: https://www.sciencedirect.com/science/article/pii/S0020025522005771.

[28] Yan Yan et al. “LSTMˆ 2 2: Multi-Label Ranking for Document Classification”. In: *Neural Processing Letters* 47 (2018), pp. 117–138.