



Een veilig

Nederland

in Europa

en de wereld



NL next level

Inhoud

Voorwoord	4
Samenvatting	6
1. Criminaliteitsbestrijding: meer preventie en meer publiek-private samenwerking	10
2. Beleid gericht op optimale cybersecurity	14
3. Een grotere en effectievere defensie-inspanning	22
4. Effectieve controle van de EU-buitengrenzen en stabilisering van de buurlanden	26
5. Naar een Investeringsplan voor Afrika	28
6. Eensgezind optreden in de EU essentieel	30
Bijlage: Financiële verantwoording	34

Voorwoord

▶ **W**e leven in een tijdperk van grote veranderingen op maatschappelijk, technologisch en economisch gebied. Tegelijkertijd is in de geopolitieke verhoudingen een revolutie gaande. Als antwoord hierop hebben wij ons *NL Next Level* programma gelanceerd; om een nieuw perspectief bieden op de toekomst. En we willen helder markeren dat we als Nederland een goede uitgangspositie hebben om de uitdagingen het hoofd te bieden. Op sommige terreinen kunnen we zelfs de leiding nemen met Nederlandse oplossingen voor wereldwijde problemen. Dat vraagt om forse investeringen en een sterk Europa. Want een aantal wezenlijke vraagstukken waarmee we ons geconfronteerd zien, kunnen we alleen gezamenlijk als EU aan. Samen moeten we perspectief bieden als antwoord op maatschappelijke vragen en zorgen die er leven.

Nieuwe veiligheidsrisico's

Een aantal nationale en internationale ontwikkelingen brengen, ieder op zijn eigen manier, nieuwe veiligheidsrisico's met zich mee: onzekerheid in de samenleving, veranderingen in de aard van de criminaliteit waaronder cybercrime, en grote instabiliteit in de internationale ontwikkelingen. De beleidsintenties

van president Trump, de agressieve opstelling van president Poetin, de aangekondigde Brexit, de opkomst van China, migratie en terrorisme plaatsen Nederland en Europa in een nieuwe, sterk veranderde wereld.

Door deze ontwikkelingen is veiligheid, meer dan voorheen, een cruciaal punt op de ondernemersagenda geworden. Samen met een sterk Europa is dit onderwerp daarom een van de pijlers van onze *NL Next Level* campagne gericht op het nieuwe kabinet. Ondernemerschap gedijt namelijk alleen bij veiligheid, stabiliteit en goede samenwerking met onze (Europese) partners. Het zijn essentiële basisvoorwaarden voor ondernemers om in de maatschappij toegevoegde waarde te scheppen en duurzame welvaart voort te brengen. Daarbij spelen ondernemers zelf ook een steeds belangrijkere rol bij het realiseren van veiligheid, al dan niet in samenwerking met de overheid.

In deze brochure, *Een veilig Nederland in Europa en de wereld*¹, geven wij onze visie op het beleid dat voor veiligheid en een sterke positie van Nederland in Europa en de wereld nodig is. De nieuwe veiligheidsrisico's, die van een andere

¹ *Een veilig Nederland in Europa en de wereld* is één van de onderdelen van het *Next Level* programma van VNO-NCW, MKB-Nederland en LTO Nederland.

orde zijn dan we tot nu toe kennen, vergen een aanpak waarbij nauwe samenwerking tussen publieke en private sector nodig is.

Niet terugtrekken achter de dijken

Bij het streven naar veiligheid is de verleiding groot om ons 'terug te trekken achter de dijken'. Die reflex is breed zichtbaar wereldwijd. Maar daar is Nederland niet bij gebaat, zo leert de geschiedenis. Voor een open maatschappij en economie als Nederland is de uitdaging juist om een goed evenwicht te vinden tussen veiligheid enerzijds en openheid anderzijds. Tussen bescherming en vertrouwen. Dat geldt op nationaal en op internationaal niveau.

Openheid en vertrouwen

Nationaal denken we bij openheid en vertrouwen aan waarden als democratie en vrijheid van meningsuiting, de rechtsstaat, de sociale markteconomie. Die waarden zijn in onze Grondwet en ook in het EU-Verdrag verankerd. Internationaal kunnen we denken aan het respecteren van het bestaande internationale stelsel en bestaande grenzen, maar vooral ook het handhaven van het open, internationale handels- en investeringsstelsel waarbij consumenten en bedrijven zeer gebaat zijn. Wij verdienen onze boterham voor een belangrijk deel over de grens. Ons land blijft vitaal door een open en nieuwsgierige blik op de wereld. Daar staan we pal voor als ondernemers.

Vijf sporen voor een veiliger en sterker Nederland

In deze agenda stellen we vijf sporen voor om Europa en de positie van Nederland daarin te versterken:

- de criminaliteitsbeheersing in Nederland en Europa op een nieuwe leest schoeien (meer accent op preventie en publiek-private samenwerking);

- de aanpak van cybercrime fors intensiveren;
- onze krijgsmacht moderniseren en een sterkere band met de industrie realiseren;
- een investeringsplan voor Afrika opzetten en uitvoeren;
- een effectieve *smart* bewaking van de buitengrenzen van Europa realiseren, omdat die essentieel zijn voor het voortbestaan van Europa zoals we dat kennen.

Op deze terreinen doen we ook concrete voorstellen voor doorbraakprojecten die overheid en het bedrijfsleven samen kunnen oppakken om zo leiderschap te nemen en innovatie te stimuleren. Naast deze vijf sporen is een essentiële randvoorwaarde voor veiligheid dat de EU meer eensgezind optreedt.

Optimisme

Als ondernemers, optimistisch als altijd, is onze overtuiging dat Nederland de uitdagingen waarvoor we ons gesteld zien aankan. Dat geldt nationaal en ook internationaal, samen met onze partners in de EU en de NAVO. Met deze concreet uitgewerkte *NL Next Level* aanpak dragen wij ons steentje bij. Laat optimisme en geloof en ons eigen kunnen zegevieren om zo te kunnen blijven groeien als samenleving.

Hans de Boer, voorzitter VNO-NCW
Michaël van Straalen,
voorzitter MKB-Nederland
Marc Calon, voorzitter LTO Nederland

Samenvatting

► De ontwikkelingen

Op het gebied van veiligheid zijn op dit moment de volgende vier ontwikkelingen van bijzonder belang:

1. Vertrouwen neemt af

We zien in onze samenleving een wijd verbreid en toenemend ongenoegen en een afnemend vertrouwen. Zorgen over de economische vooruitzichten zijn daar een oorzaak van, maar ook angst over het behoud van eigen identiteit in een samenleving van grote veranderingen. Het onbehagen leidt ertoe dat mensen zich afkeren van de bestaande 'elites', instituties als de EU en beginselen waarop onze maatschappij rust. Dit bedreigt uiteindelijk de maatschappelijke stabiliteit en heeft voor burgers en bedrijven een averechts effect.

2. Veranderende dreigingen

De aard en omvang van de criminaliteit en de

dreigingen die nationaal op ons afkomen, veranderen sterk. Nieuwe risico's komen op door de druk op de samenleving van migratie, door terrorismedreiging op *soft targets*, radicalisering en ondermijning. De criminaliteit omvat naast overvallen, inbraak, diefstal en dergelijke ook steeds meer digitale vormen, fraude en vermenging van boven- en onderwereld (ondermijning).

3. Snel stijgend belang cybersecurity

De digitalisering van de economie en de samenleving vereist dat onze cybersecurity tot de wereldtop behoort. Er is een digitale wapenwedloop gaande, waarbij kwaadaardige hackers, criminelen en in sterk toenemende mate staatsactoren steeds complexere en geavanceerdere cyberaanvallen uitvoeren. Nederland is één van de meeste gedigitaliseerde landen ter wereld en de risico's voor ons land zijn navenant.

4. Internationale ontwikkelingen

Onze binnenlandse veiligheid is niet meer los te koppelen van internationale ontwikkelingen en acties op internationaal niveau. Migratie, terrorisme en de recent weer toegenomen invloed van de geopolitiek op de internationale economische verhoudingen laten dat duidelijk zien. Onze economie is hecht verweven met de wereld. Tegelijkertijd is het in de multipolaire wereld van vandaag niet meer vanzelfsprekend dat alle grootmachten de beginselen van de internationale orde respecteren. En het is ook niet vanzelfsprekend dat de VS en de EU, die de afgelopen decennia de hoeders waren van die orde, deze onder alle omstandigheden kunnen of willen blijven handhaven.

Nieuwe initiatieven nodig!

Om Nederland verder te brengen zijn minimaal de volgende acties en projecten van vitaal belang. In de achterliggende hoofdstukken zijn deze sporen verder uitgewerkt. In totaal is voor deze opgave tenminste 1 miljard euro extra per jaar nodig.

1. Meer preventie en meer publiek-private samenwerking bij criminaliteitsbestrijding

Naast repressie moet vooral fors worden geïnvesteerd in preventie. De repressieketen biedt immers geen effectieve oplossing voor opkomende criminaliteitsvormen als fraude, afpersing, cybercrime en vermenging van boven- en onderwereld (ondermijning). Een publiek-private aanpak gericht op voorkomen is effectiever. Daarbij bieden nieuwe technologieën, zoals het uitwisselen en analyseren van data, het gebruik van camera's en fysieke en elektronische belemmeringen, extra mogelijkheden. Wij stellen daarom voor dat een vast percentage van ten minste 2,5 procent van

de begroting van Veiligheid & Justitie wordt besteed aan preventie. Nu is dat nog minder dan 1 procent. Met een voor preventie geoormerkt deel van de begroting komt er capaciteit om bewezen succesvolle preventiepilots en barrièremodellen op grotere schaal toe te passen. Door publieke partijen, private partijen en wetenschap meer te laten samenwerken kunnen meer en betere resultaten worden bereikt. Er ontstaat ruimte voor de nodige proces- en projectbegeleiders om gemeenten en ondernemers bij te staan om (ondermijnings-)locaties weer onder controle te krijgen. Verder moet de publiek-private samenwerking flink worden geïntensiveerd worden op nationaal, regionaal en lokaal niveau. Daarbij moet er ruimte zijn voor ondernemerschap.

2. Een beleid gericht op optimale cybersecurity

Het Rathenau Instituut² legde onlangs nog de vinger op de zere plek: Nederlandse overheden en bedrijven zijn onvoldoende beschermd tegen cybercrime. Daarom moet een meerjarig publiek-privaat actieprogramma met bijbehorende investeringsagenda worden opgesteld om de cybersecurity structureel te versterken. Dit vraagt om een impuls vanuit een nieuw kabinet van minimaal 100 miljoen euro extra per jaar. Bijvoorbeeld voor een Digital Trust Centre, waar branches en bedrijven terecht kunnen voor meldingen van dreigingen, advies en vragen. Nu kunnen alleen vitale infrastructuren terecht bij het Nationale Cybersecurity Centrum. Onze cybersecurity kan ook tot de beste in de wereld gaan behoren als we slimmer aanbesteden en de overheid vaker optreedt als *launching customer*. De cyberweerbaarheid moet verder worden gestimuleerd door onder meer betere informatiedeling over cyberontwikkelingen; door versterking van het

² Rapport *Een nooit gelopen race – Over cyberdreigingen en versterking van weerbaarheid*, Rathenau Instituut, maart 2017.

nationale detectie- en responsnetwerk; door ondersteuning bij het opzetten van regionale of sectorale cyber-samenwerkingsverbanden; en door de ontwikkeling van veilige hard- en software, bij voorkeur door een Europese of internationale aanpak (security by design). Ook moet het onderwijs de cyberweerbaarheid bevorderen.

3. Een grotere en effectievere defensie-inspanning

Nederland en de Europese Unie moeten over een geloofwaardig afschrikkingspotentieel beschikken nu ook de VS duidelijk van koers zijn veranderd en een grotere Europese defensie-inspanning verwachten. De Nederlandse defensie-inspanningen moeten daarom effectiever worden door modernisering van de capaciteiten. Er moet meer samenwerking op defensiegebied komen in de EU door: veel meer operationele samenwerking tussen lidstaten die zelf die stap willen zetten; door de samenwerking binnen de European Defence Agency te versterken, zodat aanschaf en gebruik van materieel zo effectief mogelijk worden; en door te zorgen dat de EU een defensie-industrie heeft die op het hoogste technologische niveau opereert. De Nederlandse defensie-industrie moet daarbij in positie worden gebracht worden om op voet van gelijkwaardigheid te kunnen concurreren op de groeiende Europese markt. Om die positionering mogelijk te maken moet de Nederlandse overheid de defensie-industrie versterken door 60 miljoen euro per jaar uit te trekken voor een intensivering op het gebied van onderzoek en ontwikkeling en door budget vrij te maken voor experimenteerruimte (Field Labs) op basis van publiek-private samenwerking. Daarvoor komt 90 miljoen euro van overheidszijde en 45 miljoen van de zijde van de industrie. Ook samenwerkingen zoals in het Fieldlab Smart Base moeten de ruimte krijgen.

4. Effectieve controle van de EU buitengrenzen

Een continent dat zijn buitengrenzen niet onder controle heeft, riskeert ook de grip op binnenlandse processen te verliezen. Een sterker engagement, een conflict mijdende aanpak en een brede aanpak in de buurlanden van de EU zijn dan ook nodig. Zo moet Europa nu werk maken van de invoering van een innovatief *smart border control* systeem aan de buitengrenzen van de EU. Het Nederlandse bedrijfsleven met zijn expertise op het gebied van moderne technieken zoals op onze havens, luchthavens en de internet exchange in Amsterdam kan hierbij een leidende rol spelen.

5. Een investeringsplan voor Afrika

In navolging van bondskanselier Merkel bepleiten wij een concreet investeringsplan voor Afrika gericht op stabiliteit en economische ontwikkeling; mét de afsluiting en invulling van effectieve migratie partnerschappen met landen uit de buurregio en mét een geïntensiveerd EU-nabuschapsbeleid en realisatie van de EFSI investeringsfaciliteit voor Afrika, zodat we groei en vooruitgang creëren. Het bedrijfsleven moet bij dit plan nauw worden betrokken. Een grotere focus van het Nederlandse en Europese beleid voor ontwikkelingssamenwerking (OS) op de buurregio is nodig, waarbij aan de ene kant wordt ingezet op het verhogen van de veiligheid en stabiliteit – waarmee een basis wordt geboden voor een ondernemingsklimaat op de lange termijn – en aan de andere kant kennis en kunde van het Nederlands bedrijfsleven wordt ingezet bij de ontwikkeling van de landen. Daartoe is een reallocatie binnen het budget van OS nodig van 1,5 miljard euro. Noodhulp moet zich meer richten op de buurregio van de EU en worden omgezet in een structureel plan voor humanitaire hulp waarbij het bedrijfsleven structureel wordt ingeschakeld. Het is zaak



Foto: Zoltan Mathe/HH

bedrijven en niet-gouvernementele organisaties (ngo's) samen te brengen om innovatieve oplossingen voor noodhulp te ontwikkelen. Initiatieven als de *Dutch Coalition for Humanitarian Innovation* kunnen hierbij als katalysator werken.

Essentiële randvoorwaarde: een meer eensgezind EU-optreden

Naast deze vijf specifieke sporen is essentieel voor de veiligheid dat de EU meer eensgezind optreedt. De instabiele internationale situatie maakt dat noodzakelijker dan ooit. Voor het Europebeleid zijn de volgende vijf zaken van belang:

- De huidige wereldsituatie noopt de EU meer dan ooit tot eensgezind optreden op

terreinen als klimaat, handel, veiligheid, migratie en financiën.

- De EU moet zich richten op concrete resultaten en een betere taakuitoefening en nu niet op vergezichten op institutionele discussies.
- De EU moet de bestaande economische agenda van de Commissie verder uitvoeren.
- De EU moet voortbouwen aan een open internationaal handels- en investeringsklimaat.
- De EU moet een sociale agenda uitwerken zodat alle EU-burgers maximaal kansen kunnen ontwikkelen.

1. Criminaliteitsbestrijding: meer preventie en meer publiek-private samenwerking

▶ Criminaliteit en algemene veiligheidssituatie veranderen

Veilig ondernemen in Europa en de wereld begint met veilig ondernemen op lokaal niveau. Een ondernemer moet erop kunnen vertrouwen dat al zijn bedrijfsmiddelen (inclusief bedrijfsgevoelige informatie) optimaal beschermd zijn. Overheden en bedrijfsleven lopen echter op het terrein van veiligheid en criminaliteitspreventie achter de ontwikkelingen aan. Dat was altijd al het geval, maar nu het tempo van ontwikkelingen hoger ligt, zijn des te meer snelheid en een flexibele en praktische 'Next Level'-aanpak nodig om de schade te beteugelen, zowel aan de publieke als aan de private kant.

De aard van de criminaliteit verandert snel. Nog maar een decennium geleden was het

tegaan van overvallen, diefstal, inbraak en graffiti speerpunt van criminaliteitsbeleid. Vandaag de dag is meer en meer sprake van bijvoorbeeld afpersing via internet en computergijzeling. Diefstal van geld, goederen en informatie in het fysieke domein bestaat nog steeds, maar is uitgebreid met diefstal via het digitale domein. Ondernijning heeft zich via vermenging van de boven- en onderwereld op verschillende niveaus genesteld. Cybercriminaliteit vormt een enorme last voor de economie (nu circa 10 miljard euro³, in 2014 al 1,5 procent BBP⁴), bij fraude gaat het om 11 miljard euro schade (bedrijven 3,7 miljard, overheid 7,3 miljard)⁵.

Ook de daders veranderen. Criminelen van nu zijn gemiddeld beter opgeleid. Ze hebben ook

³ *Cyber value at Risk in the Netherlands* (Deloitte), april 2016.

⁴ *Net Losses: Estimating the Global Cost of Cybercrime Economic Impact of cybercrime II Center for Strategic and International Studies June 2014.*

⁵ *Naar een fraudebeeld in Nederland, PWC.*

via open EU-grenzen gezelschap gekregen van ouders van elders uit Europa en via de digitale weg vanuit de hele wereld.

Tegelijkertijd zien we dat het aantal fysieke overvallen en woninginbraken de afgelopen jaren is gedaald. Het aantal overvallen bijvoorbeeld is afgenomen van 3.000 in 2009 tot ruim 1.200 in 2015, onder meer dankzij de forse intensivering van aanpak en preventie in publiek-private samenwerking.

Naast de criminaliteit verandert ook de algemene veiligheidssituatie. Er komen nieuwe risico's op. Een voorbeeld is de terrorismedreiging op *soft targets*. Recente aanslagen hebben laten zien dat doodnormale locaties doelwit kunnen zijn. Het gaat dan om plekken waar veel burgers komen, zoals voetbalstadions, markten, muziek- en winkelcentra, maar ook openbaar vervoer en luchthavens. Veiligheid in winkelgebieden, in uitgaansgebieden, op grote evenementen en op bedrijventerreinen krijgt door deze ontwikkelingen een nieuwe dimensie. Andere voorbeelden zijn de radicalisering en de druk op de samenleving als gevolg van de toestroom van vluchtelingen.

Meer preventie

De repressieketen biedt nu geen effectieve oplossing voor opkomende criminaliteitsvormen als fraude, afpersing, cybercrime en ondermijning. Als het mis gaat, moet de overheid sneller kunnen ingrijpen. Beter is echter dat we zorgen dat er überhaupt niet hoeft te worden ingegrepen. We moeten zien te voorkomen dat het mis gaat. Daarom moet er in de aanpak veel meer aandacht zijn voor preventie. Het is noodzaak

om de weerbaarheid van ondernemingen te versterken, schade te voorkomen en criminele verbanden vroegtijdig te signaleren en te onderbreken.

Preventie is in belangrijke mate de verantwoordelijkheid van een ondernemer zelf. Er zijn echter meer en complexere potentiële bedreigingen dan ooit tevoren en preventie vraagt om specialistische kennis om de juiste maatregelen te nemen en barrières op te werpen. Minder dan één procent van alle bedrijven heeft die kennis in huis en de ervaring heeft geleerd dat het inhuren daarvan slechts zeer beperkt succesvol is.

Wij stellen daarom voor dat een vast percentage van ten minste 300 miljoen euro oftewel 2,5 procent van de begroting van Veiligheid & Justitie wordt besteed aan preventie⁶. Nu is dat minder dan 1 procent.

Meer publiek-private samenwerking

De samenwerking tussen publieke sector en private sector moet flink worden geïntensiveerd; op nationaal, regionaal en lokaal niveau. Veiligheid wordt vaak nog gezien als een eerste kerntaak van de overheid, maar de overheid geeft aan dat zij het niet alleen kan en doet een dringend beroep op bedrijfsleven en burgers. Veiligheid is in toenemende mate niet alleen in handen van de overheid, maar ook van de private beveiligingsbedrijven. Denk aan bedrijventerreinen, gebouwen, evenementen, winkelgebieden, uitgaansgebieden, openbaar vervoer en luchthavens. Ook samenwerking met de sectoren financiële dienstverlening, verzekeringen, logistiek en energie biedt enorme kansen om de veiligheid te vergroten.

⁶ 100 mln voor cyber en 200 mln voor overig preventie, van onderzoek tot pilots, weerbaarheidstrainingen, borgen (bestaande en nieuwe) succesvolle zaken etc.

Publiek-privaat kan bijvoorbeeld breed worden ingezet op het wegnemen van barrières, het delen van informatie, samenwerking bij waarnemingen met technische apparatuur (*sensing*), gezamenlijk opleiden en trainen met politie, korte lijnen tussen publieke partijen en tussen publieke en private partijen, onafhankelijke voorlichting en lokale samenwerking, bewustwording en herkenning van radicalisering, screening en oog voor vitale functies in de samenleving. Daarnaast moet bij preventie veel meer gebruik worden gemaakt van technologische oplossingen. Het bedrijfsleven heeft hier vaak een voorsprong op de overheid. Een voorbeeld is de technologie die op Schiphol wordt ingezet gericht op preventie.

Ook bij de aanpak van horizontale fraude – de fraude tussen burgers, bedrijven en financiële instellingen – kan samenwerking met particuliere onderzoekers veel opleveren. De politie heeft daar nu veelal geen tijd voor.

Samenwerking zal daarom wederzijds profijt opleveren en criminaliteitsbestrijding via preventie veel effectiever maken. Daarnaast leidt samenwerking tot meer bedrijvigheid, banen en innovatie.

Er zijn veel preventieprojecten die goede resultaten laten zien, regionaal en sectoraal. Goede voorbeelden zijn de Spaanse Polder en de regio Tilburg, waar politie, stadmarinier en branches samen verzekeringsfraude, heling en witwassen tegengaan. Of hotels en politie die succesvol verschillende vormen van prostitutie aanpakken, makelaars en politie die samen henneptelers opsporen, de logistieke sector die met de politie werkt aan het opsporen van fout vervoer (drugs of heling), of een digitaal opkopersregister waarmee politie en opkopers samen heling tegengaan.

Het Keurmerk Veilig Ondernemen zorgt voor betere lokale samenwerking tussen gemeente, politie en ondernemers om zo veiligere bedrijventerreinen en winkellocaties te creëren. Het project zorgt ervoor dat partijen elkaar sneller vinden, en (dreigende) problemen worden aangepakt en niet kunnen uitgroeien. Dit tot grote tevredenheid van betrokken lokale publieke en private partijen. Het aantal aanvragen overtreft het binnen de financiën haalbare aanbod, waardoor vele gebieden nog niet bereikt zijn. De investering verdient zich dubbel en dwars terug, mede dankzij het grote hefboomeffect op lokale investeringen in veiligheid. De ervaring en het netwerk bieden tevens de uitgelezen kans om de weerbaarheid tegen opkomende vormen van criminaliteit zoals fraude, cybercriminaliteit en ondermijning te vergroten.

Wat moet gebeuren is dat deze projecten worden geïntensiveerd en uitgebreid naar andere sectoren en regio's. Bovendien moeten er structurele middelen komen voor dergelijke preventieprojecten, zodat ze niet ondanks succes weer ophouden te bestaan, maar juist structureel geborgd kunnen worden. Vergelijken met de repressie-keten is de investering beperkt in omvang en verdient zij zich ruim terug.

Innovatieve publiek-private samenwerking

Een goed voorbeeld van publiek-private samenwerking is de recent gestarte aanpak cybersecurity. Brancheorganisaties doen samen met de Haagse Hogeschool onderzoek naar de cyber(on)veiligheid in de branche, waarna een pakket van maatregelen en communicatie wordt ontwikkeld met financiële steun van de ministeries van V&J en EZ en met medewerking van diverse partijen. Branches en bedrijven kunnen daarmee op hun eigen terrein aan de slag, lokaal en regionaal kan de meer algemene informatie worden ingezet. Opgedane kennis en ervaringen kunnen weer een voorbeeld zijn voor andere preventie-verbetertrajecten.

Meer samenwerking op Europees niveau

Om het misbruik van open grenzen door de criminaliteit en het verschil in wetgeving tussen lidstaten uit te bannen, moet ook de samenwerking op Europees niveau worden versterkt. De in Den Haag gevestigde Europese organisaties Europol voor politiesamenwerking en Eurojust voor justitiële samenwerking zijn daarvoor belangrijke spelers.

2. Beleid gericht op optimale cybersecurity

▶ Nederland koploper in digitalisering

Digitalisering van de economie en samenleving gaat steeds sneller. Data worden belangrijker en omvangrijker en steeds meer apparaten zullen verbonden worden met internet. De Nederlandse economie behoort in de wereld tot de koplopers op het gebied van digitalisering. Onze digitale infrastructuur heeft zich ontwikkeld tot derde mainport. AMS-IX is één van de grootste internetknooppunten van de wereld, de breedbandnetwerken in ons land zijn uitstekend, de internetdichtheid is zeer hoog en onze bevolking is digitaal zeer vaardig en actief⁷.

Cybersecurity vraagt publiek-privaat actieprogramma met investeringsagenda

Om de vruchten van digitalisering voor economie en maatschappij te plukken, moet ook de digitale veiligheid tot de wereldtop behoren. In een digitale samenleving moeten we vast

kunnen rekenen op ongestoord functioneren van ICT-systemen en toegang tot betrouwbare informatie. Cybersecurity is een essentiële randvoorwaarde voor economische groei en welvaart en voor de digitale kwantumsprong⁸. Daarbij moet een goede balans bestaan tussen veiligheid enerzijds en het vermijden van onnodige beperkingen voor ondernemers anderzijds.

Het biedt bovendien enorme economische kansen als het Nederlandse bedrijfsleven een mondiale topospositie inneemt op het ontwikkelen van cybersecurityoplossingen en op deze wijze een disproportioneel groot marktaandeel van deze groeiemarkt weet te veroveren.

Digitale veiligheid is echter niet vanzelfsprekend. Het aantal cyberdreigingen groeit snel⁹. Cybercriminelen worden steeds professioneler, de cyberaanvallen geavanceerder en complexer.

⁷ Zie rapport *World Economic Forum 2016 en Rapport ICT Kennis & Economie 2015*, van het Ministerie van Economische Zaken en CBS.

⁸ Zie de Next Level brochure *Investeren in een digitale kwantumsprong*.

⁹ Zie het *Cybersecurity Beeld Nederland 2016*.

De dreigingen zijn vooral gericht op diefstal van geld en waardevolle informatie, maar ook op het ontregelen van systemen. Kwetsbaarheden in software vormen een reëel probleem en moeten met voorrang worden aangepakt. Het up to date houden van alle systemen is een uitdaging voor alle gebruikers. Ook Nederlandse bedrijven zijn in toenemende mate doelwit van cyberspionage. De financiële schade door cybercriminaliteit loopt voor Nederland in de miljarden euro's¹⁰.

Cybersabotage, gericht op het ontwrichten van digitale systemen met potentieel grote maatschappelijke gevolgen, wordt steeds meer een realiteit om rekening mee te houden. Voorbeelden elders in de wereld zijn de cyberaanvallen op de digitale infrastructuur van Estland en recentelijk op de energievoorziening in de Oekraïne.

Er moet een meerjarig actieprogramma met bijbehorende investeringsagenda in nauwe publiek-private samenwerking worden opgesteld en uitgevoerd om de cybersecurity structureel te verbeteren langs de lijnen van deze brochure. Het rapport *De economische noodzaak van meer cybersecurity; Nederland Digitaal Droge Voeten* – dat de ceo van PostNL, Herna Verhagen, in oktober 2016 heeft aangeboden aan premier Rutte en VNO-NCW voorzitter Hans de Boer – vormt hiervoor ook een belangrijk referentiepunt. Daarvoor moet in de begroting 100 miljoen euro worden vrijgemaakt¹¹.

Publiek-private samenwerking en eenduidige sturing nodig

De toenemende cyberdreigingen vragen dringend om effectief beleid, zodat Nederland de reputatie van een *safe place to do business* kan waarmaken en de economische en maatschap-

pelijke kansen die digitalisering biedt kan benutten. Burgers en bedrijven moeten zich veilig in de digitale wereld kunnen bewegen. Het op afstand stilleggen of overnemen van systemen door hackers, criminele organisaties en diefstal van intellectueel eigendom van onze top innovatieve ondernemingen moeten onmogelijk zijn.

De aanpak van cybercrime staat of valt met intensieve publiek-private samenwerking. Een groot deel van de ICT-infrastructuur, -kennis en -expertise is in handen van het bedrijfsleven. Overheid en bedrijfsleven zijn sterk afhankelijk van elkaar voor het verhogen van de weerbaarheid tegen cyberdreigingen, het uitwisselen van informatie en het bedenken van oplossingen. Bij een succesvolle cyberaanpak hoort ook eenduidige politieke sturing, regie en coördinatie in de uitvoering.

Op allerlei vlakken wordt reeds intensief publiek-private samenwerkt. Een voorbeeld is de financiële sector, die op het gebied van cybercrime en cybersecurity nauw samenwerkt met de overheid. Sinds tien jaar bestaat een goed functionerende FI-ISAC (Financial Services – Information Sharing and Analysis Center) voor het uitwisselen van kennis over incidenten en kwetsbaarheden. Ruim vijf jaar geleden is de Electronic Crime Task Force (ECTF) opgericht, waarin banken en politie in het kader van opsporing samenwerken. Om de samenwerking verder te verbeteren hebben de banken nu alweer drie jaar een bijna fulltime bankenliaison bij het Nationaal Cyber Security Centrum (NCSC). Dit versterkt de samenwerking tussen de financiële sector en de overheid en ook die met andere vitale sectoren.

¹⁰ Jaarlijks naar schatting circa 8-10 miljard (CSIS, Deloitte).

¹¹ Zie ook VNO-NCW, MKB-Nederland en LTO Nederland, *De Digitale Kwantumsprong*, een publicatie in de reeks van NL Next Level, oktober 2016.

Basis op orde

Overheid en bedrijfsleven moeten zich inspannen om digitaal veilig te worden. Aandacht voor cybersecurity mag geen sluitpost zijn. Voor bedrijven is betrokkenheid van het management daarbij onmisbaar. De basis moet op orde zijn bij alle bedrijven en bij alle partijen in de keten. Het midden- en kleinbedrijf moet waar nodig ondersteund worden om maatregelen te treffen. Deze maatregelen moeten in verhouding staan tot het risico dat een bedrijf loopt. Standaardisatie en praktische, concrete handreikingen zijn hierbij onmisbaar, zoals blijkt uit (branche)onderzoeken en ethische hacks. De door ondernemers gepercipieerde mate van beveiliging is nog te vaak niet in lijn met de werkelijke graad van cybersecurity. De benodigde kennis voor cyberbeveiliging op maat, zowel organisatorisch als fysiek, is zodanig complex dat het gehele bedrijfsleven, naar eigen maat en behoefte van individuele bedrijven, objectieve ondersteuning nodig heeft om de juiste maatregelen te kunnen treffen. Natuurlijk kan en moet de markt ook zelf maatregelen nemen – en dat gebeurt ook – maar de overheid heeft een belangrijke faciliterende rol, bijvoorbeeld in het organiseren van de informatiedeling tussen partijen en (internationale) overheidsorganisaties.

Versterking van de Nederlandse cyberindustrie

Veel van de huidige en toekomstige cyberproblemen zullen met behulp van innovatieve technologie kunnen worden aangepakt. Een versnelling in de ontwikkeling hiervan is nodig om een mondiale topospositie te verkrijgen en tegelijkertijd de digitale veiligheid fors te versterken.

Door de ontwikkeling van innovatieve *next-generation* beveiligingsoplossingen van internationale allure krijgt de nationale cyber-

industrie een impuls. Dit vraagt om intensieve samenwerking tussen overheid, bedrijfsleven en kennisinstellingen in de zogenaamde triple helix. De overheid moet nadrukkelijk optreden als *launching customer*, een eerste prominente investeerder en afnemer van veiligheidsproducten van Nederlandse bodem. Daarmee wordt een substantiële thuismarkt gecreëerd voor innovatie en technologische oplossingen.

Om een leidende rol te kunnen spelen op cyberterrein, moet worden geïnvesteerd in fundamenteel onderzoek. Investerings in onderzoeken naar bijvoorbeeld cryptografie en kwantumcomputing zijn essentieel voor onze internationale concurrentiepositie en hebben een aanzuigende werking op kennis en bedrijvigheid.

Ook toegepast onderzoek via SBIR waarbij de overheid aan mkb-bedrijven vraagt om met innovatieve oplossingen te komen op het gebied van cybersecurity, draagt bij aan de versterking van de nationale cyberindustrie. De regeling moet daarom worden voortgezet en versterkt, omdat deze bijdraagt aan de groei van jonge innovatieve bedrijven en nieuwe baanbrekende projecten.

Versterking van de digitale weerbaarheid van bedrijfsleven en overheid

Het versterken van de digitale veerkracht vergt inspanningen en investeringen in preventieve maatregelen, in monitoring en detectie en in een adequate respons in geval van incidenten. De aanpak moet worden toegespitst op de behoeften van de verschillende doelgroepen. Informatiedeling over cyberdreigingen, -incidenten en -kwetsbaarheden moet worden verbeterd; niet door nog meer regelgeving en meldplichten, maar door intensivering van de publiek-private samenwerking, ook over sectorgrenzen heen en ook op Europees niveau. Zowel overheid als bedrijfsleven heeft hier

een belangrijke rol. Zo moet informatiedeling door AIVD en MIVD over de werkwijze van cybercriminelen en statelijke actoren worden verbeterd. De randvoorwaarden, zoals vertrouwelijkheid, moeten op orde zijn en barrières voor informatiedeling (bijvoorbeeld strijd met privacyregelgeving) uit de weg geruimd.

Het Nationaal Cyber Security Centrum (NCSC) heeft zich ontwikkeld als een kennispin in het cyberweb. Het is van belang dat de informatie van het NCSC voor het gehele bedrijfsleven beschikbaar is. Er moet een publiek-privaat Digital Trust Centre worden ontwikkeld, waar branches en ondernemers terecht kunnen met vragen, meldingen van dreigingen en advies. Het is van belang dat de ketenweerbaarheid wordt versterkt. Het opzetten van regionale of sectorale samenwerkingsverbanden om een effectieve cybersecurity aanpak te organiseren moet worden gestimuleerd en waar nodig ondersteund.

Doorbraakproject

In de regio Eindhoven werken 25 hightech bedrijven (veelal deel van elkaars toeleveringsketen) met elkaar samen om cyberdreigingen en best practices te delen. Logische vervolgstappen zijn mogelijk een actieve deelname van het te ontwikkelen Digital Trust Centre of het NCSC, en de oprichting van een regionaal opererend Computer Emergency Response Team om kleinere hightech bedrijven uit de regio actief te ondersteunen bij cyberincidenten. Het zijn tenslotte deze hightech bedrijven waar IP beschermd moet worden tegen bedrijfsspionage. Dit is ook logisch nu Brainport behoort tot één van de Mainports in Nederland.

Het Nationale Detectie- en Responsnetwerk, waarin publiek-privaat wordt samengewerkt voor het beter en sneller waarnemen en aanpakken van digitale dreigingen en incidenten, moeten worden versterkt en uitgebreid. Bedrijven uit de vitale infrastructuur moeten met voorrang worden aangesloten. Ook dient uitbreiding met andere bedrijven die van groot belang zijn voor de verdienkracht van Nederland, mogelijk worden gemaakt.

Voor bedrijven is versleuteling van data (encryptie) een cruciaal middel om gegevens en netwerken te beschermen. Het kabinet heeft in 2016 het belang van encryptie onderschreven en dat is positief. Het gebruiken van *zero-days*¹² door statelijke actoren (politie en inlichtingendiensten) moet zo veel mogelijk worden beperkt, omdat deze vaak ook in handen komen van cybercriminelen en hierdoor de digitale wereld verzwakken. Het kabinet moet deze beleidslijnen internationaal actief uitdragen.

De overheid moet het goede voorbeeld geven door de eigen ICT op orde te brengen en cybersecurity een integraal onderdeel te maken van alle ICT-aanbestedingen (*privacy en security by design*).

Intensivering van opsporing en vervolging van cybercrime

De kennis bij politie en Openbaar Ministerie(OM) van cybercrime is beperkt en versnipperd en de capaciteit is ontoereikend. Brede politieke eensgezindheid en een budget dat aansluit bij de technologische en criminele ontwikkelingen zijn dringend gewenst om de noodzakelijke intensivering van opsporing en vervolging van cybercrime te realiseren. Voor een beter inzicht

¹² Een *zero-day* is een kwetsbaarheid in een systeem die nog niet bekend is bij de fabrikant waardoor die nog niet gerepareerd kon worden. Er is een bloeiende zwarte markt voor *zero-days*.

in de omvang van cybercrime moet de aangiftebereidheid omhoog. Hiervoor nodig zijn de inrichting van een digitaal aangifteloket, maar vooral ook capaciteit, expertise en prioritering bij de politie.

Er moet meer worden geïnvesteerd in de technische operationele capaciteit ten behoeve van de duiding van dreigingen en het coördineren van de respons daarop. Verschillende diensten, het Team High Tech Crime van de Landelijke Eenheid en de politie moeten hierop nauw samenwerken.

Ook particuliere onderzoekers kunnen hierbij een belangrijke rol spelen. Er zijn op digitaal rechercheren gespecialiseerde particuliere onderzoeksbureaus, die vaak ook al samenwerken met de nationale politie en het OM.

Meer internationale samenwerking

Miljarden apparaten, zoals auto's, medische en huishoudelijke apparatuur, zijn inmiddels verbonden met het internet. *Security en privacy by design* moeten leidende principes zijn bij de ontwikkeling van dergelijke technologische innovaties. Om de veiligheid van en het vertrouwen in deze technologische innovaties te vergroten is een gezamenlijke Europese aanpak van groot belang.

De ontwikkeling van veilige(r) hard- en software moet worden gestimuleerd. Hiertoe moet een brede dialoog met leveranciers en gebruikers worden opgezet, bij voorkeur op internationaal niveau omdat veel hard- en software uit het buitenland komt. Publiek-private samenwerking leidt tot effectieve oplossingen.

Internationale samenwerking op cybergebied is noodzakelijk, zowel in EU- als NAVO-verband als bilateraal met landen met soortgelijke

ambities. Met zijn open economie en internationale oriëntatie is Nederland bij uitstek gebaat bij een gelijk speelveld en goede internationale afspraken en samenwerking, onder meer over de noodzakelijke maatregelen ter bescherming van de netwerken, de ontwikkeling van opsporingscapaciteit en vervolging. Samenwerking met het European Cybercrime Center van Europol, EC3, moet worden versterkt en uitgebouwd. Ook nodig zijn informatie-uitwisseling en internationaal gezamenlijk opsporen.

Versterking van arbeidsmarkt, onderwijs, bewustwording

Er is een oplopend tekort aan vooral technische cybersecurity professionals. De concurrentiestrijd om deze schaarse experts is hevig. Opleidingen en arbeidsmarkt sluiten niet in alle gevallen goed op elkaar aan. Het is van belang dat de instroom naar informaticaopleidingen omhoog gaat. De bestaande aanpak, o.a. met het Techniekpact en de Human Capital Agenda ICT, moet worden versterkt. Maar het begint allemaal bij het opnemen van digitale geletterdheid in het onderwijs. Van jongs af aan moeten kinderen leren omgaan met de digitale werkelijkheid en weerbaar worden tegen de schaduwzijden. Digitale vaardigheden moeten een vast onderdeel worden van het curriculum; van basisonderwijs tot alle vormen van middelbaar onderwijs.

Verder blijft het belangrijk om via doelgerichte voorlichtingscampagnes het bewustzijn bij consumenten en bedrijven te vergroten en hen te stimuleren waar nodig maatregelen te treffen.

Veiligheid in een nieuwe wereld

De instabiliteit in de wereld neemt sterk toe. Tegelijkertijd zijn de fundamentele uitdagingen voor Nederland – veiligheid, consolidering van economisch herstel, klimaat, milieu, grondstoffenschaarste, breed maatschappelijk onbehagen – allemaal internationaal van aard. Er is dus meer noodzaak tot internationale afstemming, terwijl de voorwaarden daarvoor ongunstiger zijn. Nederland kan op de internationale uitdagingen op eigen houtje geen wezenlijke invloed uitoefenen. Dat kan ons land echter wel in het grotere kader van de EU. Nederland is deel van de EU, die deel is van een multipolaire wereld. Dat is het kader van ons internationale beleid.

De geopolitiek speelt recent opnieuw een grotere rol in de internationale economie. Geopolitiek is niet een ver-van-ons-bed show, zij raakt bedrijven direct. Bedrijfsbelangen en internationale relaties zijn immers nauw verweven. Global Value Chains kunnen alleen functioneren bij goede internationale verhoudingen. Daar kan het bedrijfsleven deels zelf voor zorgen. Het bedrijfsleven is vanwege zijn omvang en internationale belangen een belangrijke partij in de geopolitiek. Maar het heeft daarbij overheden en internationale instellingen nodig als partners. Alleen zij hebben de benodigde bestuurlijke capaciteit en instrumenten – diplomatie, inlichtingen, politie, krijgsmacht.

Voorbeelden zijn er te over: een raamwerk dat open internationale handel en investeringen mogelijk maakt; toegang tot het internationale financiële systeem; toegang tot het internet en de cloud; cybersecurity; bescherming tegen concurrentievervalsend monetair beleid; bestrijding van internationale misdaad en spionage en van piraterij in internationale vaarwegen; toegang tot grondstoffen en energie; ijkpunten bij exportcontrolebeleid in tijden van spanning; hulp bij natuurrampen; een effectief internationaal mededingingsregime en regulering van staatsbedrijven; politieke

druk op ‘schurkenstaten’ en de stabilisering van falende staten. Dit alles vraagt om een effectieve overheid.

Omgekeerd hebben de EU en haar lidstaten ook het bedrijfsleven nodig. Een welvarende unie is de basis voor een sterker Europa in de wereld.

Een multipolaire wereld

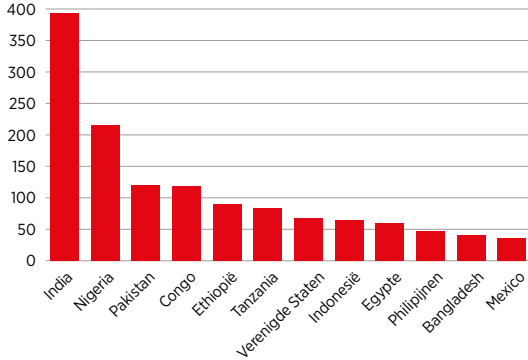
Na 2008 leidde de economische crisis versneld tot een herschikking van economische en politieke machtsverhoudingen in de wereld. Amerikaanse heerschappij maakte plaats voor multipolariteit en instabiliteit. Multipolariteit zal de wereld meer veranderen dan we nu nog denken. De multipolaire wereld van vandaag is niet simpelweg the Waning West and the Rising Rest. Ook al krimpt het Westen, het heeft nog steeds een enorm potentieel en de opkomende landen staan voor enorme opgaven. Maar Nederland en het bedrijfsleven moeten wel hun plaats vinden in een nieuwe wereld. Hoe ziet die er op dit moment uit?

De veranderende positie van de EU in de wereld: bevolkingsgroei en economische groei

De wereldbevolking groeit van 2015 tot 2050 van 7,3 naar 9,7 miljard mensen. Die groei zit voornamelijk in opkomende economieën. Samen zorgen deze landen tot 2050 voor meer dan de helft van de groei van de totale wereldbevolking. Geen enkel Europees land zit in de Top 10 van stijgers; het zijn voornamelijk Afrikaanse landen die de lijst aanvoeren.

Grootste groeiers bevolkingsomvang 2015-2050

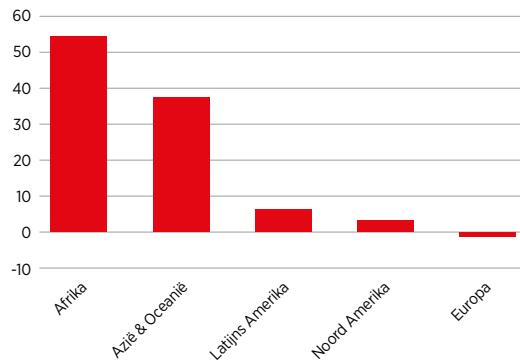
(x 1.000.000 personen)



Bron: United Nations (2015). Global Population Prospects, medium scenario

Tot 2050 is Afrika goed voor de helft van de totale groei van de wereldbevolking, gevolgd door Azië en Latijns-Amerika. In Europa krimpt de bevolking.

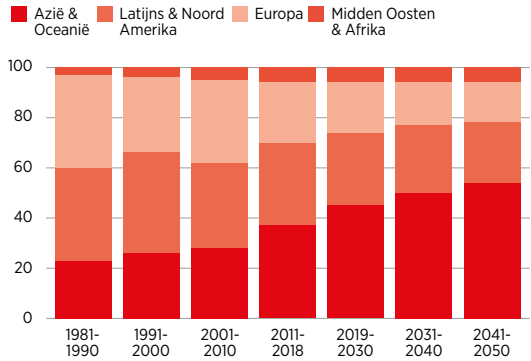
Aandeel in de groei van de wereldbevolking tot 2050 in %



Bron: United Nations (2015). Global Population Prospects, medium scenario

Azië is naar verwachting in 2050 goed voor meer dan de helft van de wereldeconomie. Ook in Afrika is de groei verhoudingsgewijs erg groot. Het verdubbelt zijn marktaandeel in de wereld. De economie van Europa, nu nog goed voor een kwart van de wereldeconomie, zal in 2050 nog maar een zesde ervan vertegenwoordigen.

Regional share of global GDP (%)



Bron: The Economist Intelligence Unit

De aangrenzende regio van de EU

De EU wordt omgeven door een zone van instabiliteit en onrust, van Sint Petersburg tot Casablanca. In het Midden-Oosten, Noord-Afrika en Sub Sahara Afrika, op luttele uren afstand van de zuidgrens van de EU, is het beeld zorgwekkend. En dat kan nog decennia voortduren. In Sub Sahara Afrika zal de bevolking tot 2050 verdubbelen. Recent optimisme over het continent verdween met de inzakkende grondstofprijzen. Omvangrijke migratiestromen van daar zijn te verwachten. Turkije doet het economisch nog goed, maar distantieert zich steeds meer van EU-waarden en daarmee van perspectief op lidmaatschap.

In Oekraïne zijn structurele veranderingen nodig. Als transformatieve power kan de EU daarbij een waardevolle partner zijn. Stabilisering en een constructieve ontwikkeling zullen echter niet mogelijk zijn zonder een vergelijk met Rusland. In Rusland zelf lijkt het onwaarschijnlijk dat de huidige machthebbers dynamische economische groei kunnen realiseren. De economie lijdt onder lage olieprijsen, economische sancties en een algemeen gebrek aan concurrentiekracht. Er zijn geen oppositiepartijen, vrije media of civil society. De overheid richt zich te weinig op economische ontwikkeling en diversificatie.



Foto: TON TOEMEN/PH

De VS

De VS is in de wereld in economisch en militair opzicht nog altijd nummer één. Maar hun relatieve gewicht neemt af en ze willen niet meer de politieagent van de wereld zijn. Dit heeft gevolgen voor de veiligheidspaplu die zij boven de EU houden. Europa zal zijn eigen defensie moeten gaan betalen. De Amerikaans economie wint aan kracht door energie-onafhankelijkheid en nieuwe technologieën en wordt opnieuw interessant voor de maakindustrie en buitenlandse investeringen. Populisme, isolationisme en het ter discussie stellen van ongelijkheid treden op de voorgrond.

China

China is een enorme macht die voor enorme uitdagingen staat. Het wil een wereldmacht worden, en onafhankelijk van het Westen. Dat komt heel zichtbaar tot uitdrukking in het OBOR initiatief, One Road, One Belt, een plan voor samenwerking en massieve infrastructuurontwikkeling in meer dan 60 landen, van Beijing via Centraal Azië naar Piraeus, en van China door de Indische Oceaan naar Afrika. De schaal van het

plan is gigantisch. De Chinese economie verschuift qua oriëntatie van export naar binnenlandse bestedingen en technologische autonomie in 2025.

Positieve internationale ontwikkelingen

Bij alle uitdagingen zijn er ook belangrijke positieve ontwikkelingen. De recente economische crisis was ongekend, maar het internationale systeem bleef intact. De Verenigde Naties bereikten overeenstemming over de Sustainable Development Goals (SDG). Er kwam een nieuw wereldwijd klimaatakkoord. De World Trade Organization bereikte een akkoord over douanevereenvoudiging. De EU voerde substantiële hervormingen door om banken en de euro te versterken en sloot een migratieakkoord met Turkije. Dus ook in moeilijke tijden loont het om in internationale samenwerking te investeren. En technologische veranderingen boezemen sommigen angst in, maar leiden ook tot ongeken-de mogelijkheden en kansen. Burgers verwachten dat het bedrijfsleven de technologische ontwikkelingen zal omzetten in belangrijke innovaties.

3. Een grotere en effectievere defensie-inspanning

► We staan voor echte dreigingen

Na de Koude Oorlog is er in het kader van het 'Vredesdividend' steeds meer bezuinigd op defensie. Nederland en de andere EU-landen konden zich de luxe permitteren om minder aan defensie uit te geven omdat de wereldsituatie een aantal jarenlang geen specifieke bedreigingen voor de EU opleverde. Bovendien waren de VS altijd bereid om het leeuwendeel van de kosten van het NAVO-budget voor hun rekening te nemen.

Beide omstandigheden zijn geheel veranderd. De VS verwachten van Europese landen een aanzienlijk grotere bijdrage om de defensie van Europa te betalen. En met de nieuwe veiligheidssituatie in Europa – de Russische annexatie van de Krim, de inmenging in Oost Oekraïne en de instabiliteit van veel landen in het Midden-Oosten, Noord-Afrika en Sub Sahara Afrika – staat Europa in zijn onmiddellijke omgeving voor echte dreigingen. Dit vraagt om een nieuwe aanpak.

Verhoging van de Nederlandse defensie-inspanning

De toestand van onze krijgsmacht na alle opeenvolgende bezuinigingen is zorgelijk. Investerings zijn de komende jaren hard nodig. De instabiliteit in de buurlanden van de EU vraagt om een geloofwaardig afschrikkingspotentieel. Aanvoerlijnen voor de koopvaardij moeten worden beveiligd. En Nederland, als knooppunt van datastromen, heeft een toenemend belang bij cybersecurity, nu cyberaanvallen door andere staten snel toenemen.

De Nederlandse defensie-inspanningen moeten daarom effectiever worden, en het budget moet omhoog. De Nederlandse defensiebegroting voor de jaren 2016 en 2017 bedraagt ruim 8 miljard euro. Dit is circa 1,1 procent van het bnp, terwijl de NAVO-doelstelling 2 procent BNP is. Het Europese gemiddelde van de NAVO-landen is 1,4 procent BNP. De recente verhoging van de Nederlandse defensiebegroting met circa 550 miljoen euro was noodzake-

lijk om de basisgereedheid van de krijgsmacht te verhogen, maar vult dat gat niet.

Veiligheid vereist meer Europese samenwerking

De realiteit is dat geen enkel EU-land alleen in staat is voor zichzelf voldoende veiligheid te scheppen. Dat kan alleen met een collectieve inspanning. Wij moeten als lid van de internationale gemeenschap onze verantwoordelijkheid nemen, in de NAVO en in de EU. Als wij als land erop willen rekenen dat onze bondgenoten ons in een crisissituatie bijstaan, dan moeten we ook zelf onze verplichtingen nakomen.

De EU moet nog een flinke slag maken. Het revolutionaire samenwerkingsmodel van Europa is gestoeld op *soft power*. Dat heeft ertoe bijgedragen dat we in Europa al meer dan vijftigjaar in vrede leven. De werkelijkheid dwingt nu te accepteren dat de EU haar *soft power* moet schragen met *hard power*. Daarbij heeft de EU echter een dubbele handicap te overwinnen: interne verdeeldheid en het gebrek aan *hard power*.

Gezamenlijk kunnen de EU-landen een geloofwaardig afschrikingspotentieel realiseren. Daarom moeten zijn veel meer samenwerken op defensiegebied. Niet door een eindeloze discussie te starten over een gezamenlijk Europees leger, maar door op korte termijn een aantal belangrijke concrete stappen te zetten:

- Veel meer operationele samenwerking mogelijk maken tussen lidstaten die zelf die stap willen zetten.
- Samenwerking binnen de European Defense Agency verbeteren, zodat aanschaf en gebruik van materieel zo effectief mogelijk worden, zo kan het defensiebudget optimaal worden aangewend.
- Het in stand houden van een zelscheppende defensie-industrie die op het hoogste techno-

logische niveau opereert. Zonder zo'n industrie kan Europa strategisch niet autonoom zijn in de wereld, maar is zij afhankelijk van anderen voor haar veiligheid.

Sterkere positionering van de Nederlandse defensie-industrie

Als wij op defensiegebied meer gaan samenwerken in Europees verband, moeten we zorgen dat de Nederlandse defensie-industrie in positie wordt gebracht om op voet van gelijkwaardigheid te kunnen concurreren op de groeiende Europese markt voor defensieaanbestedingen.

Defensie speelt een belangrijke rol in economisch opzicht. Defensie zorgt voor directe werkgelegenheid en is een belangrijke opdrachtgever voor het bedrijfsleven. De defensie-industrie is kennis- en innovatie intensief. Zij bestaat in Nederland vooral uit civiele ondernemingen en onderzoeksinstellingen die in militaire productie gespecialiseerde afdelingen hebben. Van de omzet wordt 70 procent geëxporteerd.

Kerngegevens van de Nederlandse defensie- en veiligheid gerelateerde industrie

Aantal bedrijven: 651

Defensie- en veiligheid gerelateerde omzet 2014:

€ 4,54 miljard

Defensie- en veiligheid gerelateerde omzet als % van de totale omzet: 15 procent

Defensie- en veiligheid gerelateerde export 2014:

€ 3,09 miljard

Aantal defensie- en veiligheid gerelateerde

arbeidsplaatsen: 24.800

waarvan aantal defensie- en veiligheid gerelateerde

R&D-arbeidsplaatsen: 7.995

Bron: Triarii 2016

Voor civiele aanbestedingen gelden er in de EU strikte regels voor transparantie. Maar voor defensie aangelegenheden is het mogelijk om vanwege de nationale veiligheid opdrachten te gunnen aan enkel nationale bedrijven (*security of supply*). Veel landen besteden het overgrote deel van hun defensiebudget aan opdrachten voor nationale bedrijven; Frankrijk en Zweden zijn hier goede voorbeelden van. Daarnaast worden er in Frankrijk bijvoorbeeld afspraken gemaakt dat het grootbedrijf ook het nationale mkb inschakelt. Het is dus voor Nederlandse bedrijven heel lastig om buiten de nationale grens een opdracht binnen te halen.

In Nederland wordt er relatief minder aan het nationale bedrijfsleven gegund dan in veel andere EU-landen. Dit geldt ook voor 'civiele' producten bij defensie: de huidige Nederlandse uniformen worden bijvoorbeeld in Azië ingekocht, terwijl 's werelds meest geavanceerde textielontwikkelaar in Nederland is gevestigd. Overigens is er voor civiele aanbestedingen onder de Europese Aanbestedingswet ook slechts sprake van 3,1 procent grensoverschrijdende aanbestedingen. Op het terrein van Europese aanbestedingen valt dus nog een wereld te winnen.

De positie van de defensie-industrie kan op twee manieren worden versterkt:

Positie in Nederland

De positie in Nederland moet verstevigd worden. De defensie-industrie is gespecialiseerd en bestaat uit een beperkt aantal bedrijven. Ook het aantal opdrachtgevers (landen en internationale samenwerkingsverbanden) is beperkt. Het is een zeer gespecialiseerde markt, met een wederzijdse afhankelijkheid van opdrachtgevers en opdrachtnemers. Daarbij kan de overheid markten creëren door als launching

customer op te treden. Dat is ook nodig om daarna te kunnen exporteren.

Dit vereist dan wel een goede samenwerking tussen opdrachtgever en opdrachtnemer. Om die kansen te vergroten, moeten Defensie als opdrachtgever en het bedrijfsleven in de toekomst beter samenwerken. Die samenwerking moet al in een vroege fase van het project starten, multidisciplinair zijn en gebaseerd op innovatief partnerschap. Indien opdrachten van Defensie door buitenlandse ondernemingen worden uitgevoerd, verdwijnt hiermee veel kennis en innovatie de grens over.

Succesvolle samenwerking in Field-lab Smart-base

Een mooi voorbeeld van hoe Defensie en marktpartijen kunnen samenwerken is het Field-lab Smart Base. Dat is een experimenteeromgeving gericht op het vinden van nieuwe oplossingen voor de inrichting van bases en kampementen in het buitenland. Het is een samenwerking tussen FME, VNO-NCW, MKB-Nederland en vele bedrijven. Het initiatief is goed ontvangen door zo'n 300 geïnteresseerde mkb-bedrijven en heeft voorstellen opgeleverd – soms onsollicited, die minstens zo interessant zijn – variërend van 3D-printen tot voedingsoplossingen, van slimme toegangscontrole tot waterbesparing en van energieneutraliteit tot slimme beschermingsopties.

Positie in de EU

Ten tweede moet de Nederlandse defensie-industrie Europees gepositioneerd worden. Daarvoor zijn twee zaken van belang:

1. Behoud van compensatieorders; bij de evaluatie van de herziening van de Europese Defensie Procurement Richtlijn wordt vanuit de Europese Commissie druk gezet op het meer openbreken van de Defensiemarkt.

Daarbij wil de Commissie compensatie-orders uitbannen. Dat zal vooral nadelig uitpakken voor kleinere lidstaten als Nederland. Voordat de Europese defensie-aanbestedingenmarkt echte openheid kent, moet dit instrument niet worden opgegeven.

2. De Nederlandse defensie-industrie moet volwaardig kunnen deelnemen aan de grote Europese R&D programma's voor defensie die nu worden opgezet.

Doorbraakproject defensie-industrie

Intensievere samenwerking tussen Defensie en de industrie bij de ontwikkeling en inkoop van producten, diensten en instandhoudingsvormen leidt tot ecosystemen waarmee innovaties van defensiecapaciteiten sneller door de krijgsmacht kunnen worden benut. Daarbij leidt het optreden van de overheid als *launching customer* tot nieuwe exportkansen. Om hieraan vorm te geven zijn twee actielijnen geïdentificeerd:

1. Intensivering voor onderzoek en ontwikkeling van 60 miljoen

Op dit moment besteedt defensie 1 procent van haar budget aan R&D, de helft van de norm van het Europese Defensie Agentschap (EDA) van 2 procent. Hierdoor kan onvoldoende invulling worden gegeven aan investeringen in de prioritaire technologiegebieden die in de Defensie Industrie Strategie (DIS) zijn beschreven. Met een hoger R&D-budget wordt innovatie aangejaagd door verregaande samenwerking tussen enerzijds Defensie en anderzijds bedrijven en kennisinstellingen. Hiermee kan Defensie beschikken over de laatste stand der technologie en innovaties en wordt het exportpotentieel van veiligheidsgerelateerde producten en diensten versterkt.

2. Budget voor experimenteerruimte op basis van PPS van 90 miljoen euro aan overheidszijde en 45 miljoen euro aan de kant van de industrie

Om van R&D te komen tot nieuwe innovatieve producten met Defensie als eerste afnemer moeten (financiële) knelpunten in de keten van behoeftestelling, ontwikkeling tot en met inkoop in een vroegtijdig stadium integraal worden geadresseerd. Het optreden van Defensie als *launching customer* kan worden gefaciliteerd door zogenaamde *fieldlabs* (experimenteerruimtes) op te zetten. Het doel is een gewenst product te ontwikkelen dat Defensie wil en gaat afnemen. Daarnaast stelt dit de industrie in staat om zich te positioneren voor buitenlandse afnemers. Defensie als *launching customer* versterkt hierdoor zowel het innovatieve karakter van Defensie als het verdienvermogen van de Nederlandse economie en functioneert als motor voor kennisopbouw en innovatie. Van een goedgekeurd *launching customer*-project wordt tweederde gefinancierd door de overheid (Defensie en Economische Zaken), eenderde komt voor rekening van de betreffende industriepartij(en).

4. Effectieve controle van de EU-buitengrenzen en stabilisering van de buurlanden

► Internationale veiligheid vraagt meer dan defensie

Een duurzame internationale veiligheidsaanpak vraagt meer dan alleen defensie en strekt zich uit tot het realiseren van de *Sustainable Development Goals* door het bevorderen van stabiliteit, economische groei en maatschappijontwikkeling in onze buurlanden via onder meer ontwikkelingshulp en noodhulp. Kortom, een aanpak van veiligheid en ontwikkeling.

Concreet betekent dit voor Nederland en de EU dat enerzijds moet worden ingezet op een effectievere en vooral ook slimmere bescherming van de buitengrenzen van Europa en anderzijds op economische ontwikkeling in vooral de zuidelijke buurregio van de EU, mede door deze landen toegankelijker te maken voor het Nederlandse bedrijfsleven.

Smart Border Control systeem aan de EU-buitengrenzen

Migratiestromen naar de EU komen vooral uit de zuidelijke buurregio van de EU en uit Sub-Sahara Afrika. De situatie in tal van landen daar is toenemend instabiel door politieke onrust in en tussen landen, economische stagnatie en de gevolgen van klimaatverandering. Terwijl juist daar de mondiale bevolkingsgroei – de wereldbevolking groeit van 7,5 miljard naar bijna 10 miljard mensen in 2050 – de komende decennia zal plaatsvinden. De problemen zullen de komende decennia niet opgelost worden. We moeten er daarom rekening mee gehouden dat vluchtelingen de komende jaren naar de EU zullen blijven komen.

Grensbeleid is de link tussen externe en interne veiligheid. De grote migratiestromen van de

afgelopen tijd laten zien dat Europa zijn grenzen niet onder controle heeft. Het grensbeleid is te veel overgelaten aan de EU-lidstaten zelf. Een door de Europese Commissie voorgestelde Europese aanpak is lang tegengehouden door de lidstaten. In 2014 is de Frontex-organisatie in het leven geroepen, maar deze had te weinig bevoegdheden, personeel en budget om effectief te kunnen optreden. Sinds oktober 2016 is de *European Border and Coast Guard* operationeel. Dat is een grote verbetering. De EU kan nu lidstaten met een EU-buitengrens effectief ondersteunen als zij de grensproblemen zelf niet aankunnen.

De uitdagingen aan de Europese buitengrenzen zijn nog niet ten einde. Weliswaar zijn de vluchtelingenstromen in 2016 substantieel afgenomen na het akkoord tussen de EU en Turkije, maar de migratiedruk in de buurlanden is nog steeds groot en mensensmokkelaars zoeken naar alternatieve wegen. In Italië is dat duidelijk merkbaar. Eind 2016 kwamen daar recordaantallen vluchtelingen aan. En de potentiële vluchtelingenstromen die uit Afrika richting de EU zouden kunnen komen, zijn enorm.

Om de EU-buitengrenzen onder controle te krijgen zijn innovatieve oplossingen nodig. In de eerste plaats dient een *Smart Border Control*-systeem aan de buitengrenzen van de EU gerealiseerd te worden, met slimme hightech faciliteiten op basis van nieuwe technologie om vluchtelingenstromen op te vangen, te registreren en in goede banen te leiden. Een veelheid aan nieuwe technologieën moet daartoe worden ontwikkeld. Dit moet een gezamenlijk Europees project worden, waarbij het Nederlandse bedrijfsleven een belangrijke rol kan

spelen bij de ontwikkeling van de benodigde hightech faciliteiten.

In de EU-begroting wordt 480 miljoen euro vrijgemaakt voor vierjaar (drie jaar voor ontwikkeling en uitrol en een jaar voor inwerkingtreding) voor een *Smart Border Control*-systeem. Dit is alleen voor het Entry en Exit Systeem en het laten samenwerken van de ICT-systemen (wat samen het Smart Borders-voorstel van de Europese Commissie uit 2013 vormt)¹³.

¹³ Bron: *Smart Borders revisited: an assessment of the Commission's revised Smart Border proposal*, studie van het Study Department van het Europese Parlement uit 2016.

5. Naar een Investeringsplan voor Afrika

► **D**e Duitse Bondskanselier Merkel heeft terecht gepleit voor een Marshallplan voor onze buurlanden ten zuiden van de EU. Er is namelijk meer nodig dan het ontwikkelen van een systeem dat de buitengrenzen van de EU op een slimme manier kan bewaken. Uiteindelijk moet worden bereikt dat mensen uit de naburige regio in eigen land voldoende perspectief hebben, zodat ze niet meer de stap willen zetten om richting de EU te trekken.

In juni 2016 kondigde de Europese Commissie aan daartoe Migratie Partnerschappen met individuele landen in de buurregio te gaan afsluiten. Deze zijn zowel gericht op oplossingen op kortetermijnoplossingen als op een fundamentele aanpak om de grondoorzaak van migratie weg te nemen. Momenteel worden er partnerschappen met vijf landen uitgewerkt:

Niger, Nigeria, Senegal, Mali en Ethiopië. Dit verdient een grote en steviger impuls, omdat groei de enige weg is naar een toekomst in eigen land. Een serieus uitgewerkt investeringsplan voor Afrika verdient daarom navolging. Het aanpakken van de grondoorzaken van migratie vraagt immers om een sterk Europees nabuurschapsbeleid dat stabiliteit verbetert, onder meer door economische ontwikkeling te bevorderen. Daarbij moet het Nederlandse bedrijfsleven worden ingezet. Het kan bijdragen aan de stabilisatie van de zuidelijke buurregio door het versterken van de private sector daar en het opbouwen van een ondernemingsklimaat. Het voorstel van de Europese Commissie om een EFSI-faciliteit voor Afrika in het leven te roepen, past goed in dit kader en moet daarom worden gerealiseerd.

Focus van het Nederlandse en Europese OS-beleid op de nabuurregio

Gezien het directe belang van de EU bij stabilisatie in de buurregio, moet de Nederlandse en Europese ontwikkelingssamenwerking zich meer gaan richten op de instabiele buurregio van de EU waar vluchtelingenstromen vandaan kunnen komen. Daarbij moet ook het bedrijfsleven betrokken worden.

De dubbele doelstelling van het beleid van hulp en handel is de economische ontwikkeling in ontwikkelingslanden en opkomende markten te versterken en deze landen toegankelijker te maken voor het Nederlandse bedrijfsleven. De verbinding van de ontwikkelingshulp- en de handelsagenda kan worden geïntensiveerd door:

- Het verbeteren van de randvoorwaarden voor het lokale ondernemingsklimaat en een gerichte aanpak van corruptie.
- Het bevorderen van open markten, vrijhandel en verduurzaming van de handels- en investeringsketens.
- Een slim, concurrerend financieringsinstrumentarium voor export en investeringen en een faciliteit voor vroege fase projectontwikkelingsfinanciering.
- Ondersteuning van het lokale mkb en het faciliteren van bilaterale business netwerken.
- Inzetten op het bereiken van de Sustainable Development Goals, waarbij de verdienmodellen van het bedrijfsleven worden verbonden met de maatschappelijke uitdagingen waarvoor de wereld staat via de aanpak *global challenges, Dutch solutions*.

Er zal binnen het Nederlandse OS-budget 1,5 miljard euro gealloceerd moeten worden voor dit investeringsplan voor Afrika.

Ook innovatie in de noodhulp

Er zijn inmiddels wereldwijd 60 miljoen vluchtelingen en nog eens 20 miljoen ontheemden. Dat aantal is in tien jaar tijd verdubbeld en de kosten van noodhulp zijn verdrievoudigd. Dat heeft onder meer te maken met het klimaatprobleem, conflicten binnen landen en het gegeven dat noodhulpverlening in stedelijke gebieden een stuk lastiger is dan op het platteland. Als de hulp niet op een andere manier wordt ingevuld, lukt het niet meer om die stroom op te vangen. Ook de noodhulp kan zich meer richten op de buurregio van de EU om het ontstaan van vluchtelingenstromen te voorkomen.

Noodhulp moet worden omgezet in een plan voor humanitaire hulp waarbij het Nederlandse bedrijfsleven structureel wordt ingeschakeld. Het is noodzakelijk bedrijven en ngo's samen te brengen om innovatieve oplossingen voor noodhulp te ontwikkelen. De *Dutch Coalition for Humanitarian Innovation*, een initiatief van het ministerie van Buitenlandse Zaken, Rode Kruis, Unicef, Care, VNO-NCW en de gemeente Den Haag, kan hierbij een initiatief zijn dat een katalyserende werking heeft.

6. Eensgezind optreden in de EU essentieel

▶ **N**aast de vijf genoemde specifieke sporen is essentieel voor de veiligheid dat de EU meer eensgezind optreedt. De instabiele internationale situatie maakt dat noodzakelijker dan ooit.

De EU als instrument voor veiligheid

De ingrijpende ontwikkelingen die zich internationaal voordoen, zullen gevolgen hebben voor het EU-beleid, het defensiebeleid, het internationale belastingbeleid, het WTO-beleid en allerlei andere terreinen. De grote internationale uitdagingen waar Nederland voor staat hebben allemaal gevolgen voor veiligheid en stabiliteit. Nederland alleen heeft niet de schaal om daarop invloed te kunnen uitoefenen. In het kader van de EU kan Nederland echter wel degelijk participeren en invloed uitoefenen. De EU is dus een belangrijke instrument voor ons om de internationale veiligheid te vergroten.

Samenwerking versterken

Ten behoeve van de veiligheid is van groot belang dat Europa meer eensgezind optreedt. Te denken valt aan betere samenwerking tussen inlichtingendiensten, Europol en Eurojust, maar ook aan gezamenlijke productstandaarden in verband met cybersecurity, of het voorkomen van oneigenlijke concurrentievervalsingen. En natuurlijk aan Europese defensiesamenwerking. Nederlands engagement in de EU draagt dus bij aan onze veiligheid. Een aantal aspecten van EU-beleid (defensiesamenwerking, grenscontroles, nabuurschapsbeleid, ontwikkelingssamenwerking en noodhulp) komt elders in deze brochure aan de orde. Ook Europees beleid op andere terreinen zoals klimaatverandering of grondstoffenbeleid heeft een directe impact op veiligheid.

Eensgezind optreden is ook nodig om te voorkomen dat de EU de speelbal wordt van andere wereldmachten. De EU moet er alert op zijn niet ten prooi te vallen aan verdeel-en-heers-

beleid van andere landen. Dit is ook een direct Nederlands belang.

We zien nu de paradox dat terwijl internationaal engagement belangrijker is dan ooit, en de EU dus belangrijker is dan ooit, de publieke opinie zich steeds meer naar binnen richt. De wijdverbreide eurosceptis verzwakt de autoriteit van de EU om internationaal haar economische en politieke belangen te behartigen. Wij zullen het belang van Europese eensgezindheid en samenwerking nadrukkelijk moeten uitdragen in Nederland. Ook afzonderlijke bedrijven kunnen op basis van hun ervaringen een waardevolle rol in dit debat spelen.

Focus op concrete resultaten en betere taakuitoefening

De publieke aandacht voor de crisis ontnemt veelal het zicht op de concrete resultaten die de EU de afgelopen jaren tot stand heeft gebracht en waar zij op dit moment aan werkt.

Europese successen

De EU heeft vrede en verzoening gebracht, een Interne Markt die gemak voor bedrijven en welvaart en keuzevrijheid voor burgers brengt, een landbouwbeleid dat onze landbouw aan de top van de wereld heeft gebracht, een wereldleidersrol op milieugebied, een grote vermindering aan administratieve lasten doordat voor honderden onderwerpen 28 nationale regelingen zijn vervangen door één Europese, een handelsbeleid dat bepalend is geweest voor de wereldwijde handelsliberalisering van de afgelopen halve eeuw, een globaliseringsbeleid dat meer dan waar ook ter wereld rekening houdt met burgerbelangen. Maar ook concrete zaken voor de burger zoals de afschaffing van roaming, verlaging van prijzen voor vliegreizen en verlaging van hoge creditcardtarieven. En een zeer sterke vermindering van vluchtelingenstromen in 2016 waar niemand in januari van dat jaar op had durven hopen.

Op dit moment werkt de EU aan tal van initiatieven die nodig zijn voor bedrijven: een akkoord met de VS over de privacyregels voor dataverkeer, een uitwerking van de OESO-regels voor belastingontwijking, nieuwe regeling voor het Europese systeem voor emissiehandel ETS, afspraken met China over handelsbescherming, regelgeving over geoblocking en de kapitaalmarktunie.

Het Europese debat verdient een constructievere toon. Maar het is wel nodig dat bestaande EU-taken beter worden uitgevoerd en dat de EU beter gaat leveren op onderwerpen waar burgers en bedrijven zich terecht zorgen over maken, zoals de veiligheidssituatie. De EU moet de voedingsbodemp van eurosceptis en sociale desoriëntatie aanpakken. De EU en de lidstaten moeten – en kunnen – bewijzen dat een gezamenlijk beleid voor de Europese volkeren meer vrijheid, veiligheid, welvaart en stabiliteit brengt dan een ad hoc samenwerking van min of meer onafhankelijke staten. Ondanks de verschillen tussen de lidstaten en ondanks de bestaande eurosceptis moet er meer slagvaardigheid komen.

Vier hoofdlijnen voor EU-beleid

Voor een nieuwe koers van de EU stellen de ondernemingsorganisaties vier hoofdlijnen voor:

1. Nieuw EU-beleid vraagt nu niet om vergesichten of institutionele discussies. Burgers verwachten dat de EU concrete resultaten bereikt met de middelen die zij heeft.
2. De Europese Commissie moet haar bestaande economische agenda verder uitvoeren. Die is in overleg met het bedrijfsleven tot stand gekomen en zit goed in elkaar. De agenda bereidt voor op grote veranderingen in onze samenleving en economie als gevolg van onder meer de nieuwe technologieën (zie kader).

3. De EU moet verder bouwen aan het open internationale handels- en investeringsbeleid waarop de EU gegrondvest is.
4. Naast economisch beleid moet de EU ook een sociale agenda uitwerken, zodat alle Europese burgers maximaal kansen kunnen ontwikkelen en toegerust worden met de vaardigheden die nodig zijn op de arbeidsmarkt van de toekomst.

Europese wetgeving onontbeerlijk voor nieuwe technologie

De grote technologische veranderingen (big data, robotica, autonome transportmiddelen, drones, 3D-printing, biotechnologie, nanotechnologie, human augmentation) vragen om weg- en regelgeving om de maatschappij en de economie van de toekomst te formateren. Het is belangrijk voor bijvoorbeeld toekomstige productstandaarden, kosten, concurrentieverhoudingen en aansprakelijkheid dat deze wetgeving in heel de EU gelijk is en dat de lidstaten gezamenlijk deze regels vaststellen. EU-regels zijn vaak het kader voor aanvullende nationale wetgeving.



Bijlage: Financiële verantwoording

▶ **I**n het kader van NL Next Level hebben VNO-NCW, MKB-Nederland en LTO Nederland een investeringsprogramma uitgewerkt (zie Investeren in de Transformatie van Nederland, juni 2016). Door gerichte publieke investeringen kan een veelvoud aan extra private investeringen worden losgetrokken voor de grote transitie waar we voor staan. Op het gebied van veiligheid is onderstaande financiering noodzakelijk om Nederland naar een next level te brengen. Dit kan binnen de kaders van Maastricht en hiervoor is de financiële ruimte aanwezig.

Daarnaast is een reallocatie van 1,5 miljard euro binnen het OS-budget nodig om de realisering van het investeringsplan voor Afrika mogelijk te maken.

In de EU-begroting wordt 480 miljoen euro vrijgemaakt voor vier jaar (drie jaar voor ontwikkeling en uitrol en een jaar voor inwerkingtreding) voor een Smart Border Control systeem. Dit is alleen voor het Entry en Exit Systeem en het laten samenwerken van de ICT-systemen (wat samen het Smart Borders voorstel van de Europese Commissie uit 2013 vormt).

Extra benodigd

1. Een vast percentage van 2,5 procent van de begroting van Veiligheid & Justitie moet worden geoormerkt voor preventie (nu 1 procent).
2. 100 mln euro per jaar voor een meerjarig actieprogramma met bijbehorende investeringsagenda om cybersecurity structureel te versterken.
3. Tenminste 1 mrd euro extra voor defensie, structureel per jaar.
4. 60 mln euro voor extra R&D bij Defensie en 135 mln euro op PPS-basis voor experimenteerruimte (field labs) bij Defensie.

**‘We moeten
het aanpakken
van nieuwe
veiligheidsrisico’s
combineren met
een open blik
op de wereld’**

WWW.NL-NEXTLEVEL.NL

**© VNO-NCW, MKB-NEDERLAND, LTO NEDERLAND
MEI 2017
ONTWERP: LINK DESIGN
COVER FOTO:
DAVID ROZING/HH, TON TOEMEN/HH**

NL next level