LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Universiteit Leiden

Het Chinese technologiebeleid en de Nederlandse Chinanotitie

Rogier Creemers | Januari 2020

Samenvatting

Sinds 2014 heeft de Chinese regering haar intenties op het vlak van digitale technologie verscherpt en haar beleidsvorming versneld. Met als doel het worden van een "cybergrootmacht", heeft Beijing nieuwe overheidsstructuren opgebouwd en een waslijst aan beleids- en regelgevende stappen geïnitieerd. Aan de ene kant gaan deze over een breed gedefinieerde vorm van cybersecurity, die niet alleen de integriteit van technische systemen en data behelst, maar ook zaken als informatieveiligheid en technologische afhankelijkheid van andere landen, met name de VS. Anderzijds draagt dit beleid ook bij aan "informatisering": het gebruik van digitale technologie voor het verbeteren en transformeren van maatschappelijke, economische en politieke processen. Op militair vlak investeert China eveneens in digitale technologie. Deze investeringen lijken vooral defensief van aard, en zijn nog niet goed ingebed in strategische en tactische doctrine. Internationaal gezien bevond China zich recentelijk nog in het kielzog van Rusland, maar inmiddels laat het land steeds nadrukkelijker van zich horen op het gebied van digitale technologie. China's nieuwe houding wordt voornamelijk gekenmerkt door een kritische opstelling tegenover de zogeheten Amerikaanse hegemonie en tegelijkertijd het voornamelijk bepleiten van de belangen van ontwikkelingslanden. Soevereiniteit, het recht en de capaciteit van landen om cyberspace naar eigen inzicht te ontwikkelen, is hierbinnen China's belangrijkste principe. Desondanks zoekt China internationaal ook toenadering, met name op het vlak van data-uitwisseling met de buitenwereld.

Dit Chinese beleid raakt op talrijke en complexe manieren de Nederlandse belangen. Wat betreft de Chinese markt zijn er vragen over de dominante rol van de staat hierbinnen, evenals de markttoegang voor Nederlandse en Europese bedrijven. Ook bedrijfsspionage, kennisoverdracht, *dual use* technologie en natuurlijk mensenrechtenvraagstukken blijven relevant. In Nederland zelf vormt de toenemende aanwezigheid

van Chinese spelers een uitdaging, waarvan Huawei het meest uitgesproken voorbeeld is. Daarnaast zijn er ook vragen over de mate waarin Chinese e-commerce bedrijven mogelijk aan oneerlijke concurrentie doen en in hoeverre Chinese investeringen kunnen leiden tot het verlies van binnenlandse knowhow. Ook ontmoeten Nederland en China elkaar in derde landen. Onder andere via projecten als de Digitale Zijderoute probeert China een grotere markt te creëren voor haar eigen producten, en de buitenlandse steun voor haar internationale doelstellingen te verbreden. In de diplomatieke context betreffen de belangrijkste vraagstukken tussen Nederland en China de normering van staatsgedrag. Dit debat bevindt zich echter in een impasse, mede vanwege de groeiende spanning tussen China en de VS.

Dit rapport doet geen aanbevelingen over wélke beslissingen Nederland ten aanzien van deze vraagstukken dient te nemen, maar het stelt wel maatregen voor die snel zullen moeten worden toegepast om het nemen van de meest effectieve keuzes mogelijk te maken. Ten eerste moet Nederland, samen met haar Europese partners, een eigen strategische koers kiezen en varen. Realiteitszin is hierin belangrijk. De mate waarin Nederland en Europa Chinees gedrag kunnen beïnvloeden is klein, en het verdient dus de voorkeur de samenwerking pragmatisch te structureren. Gezamenlijk optrekken, vooral binnen de EU, is daarbij essentieel. Ook moet de relatie met China gezien worden in het kader van de trans-Atlantische verhouding, waarbinnen de strategische autonomie van Nederland en Europa opnieuw benadrukt dient te worden. Ten tweede moet Nederland de vraagstukken specifieker benaderen en minder terugvallen op generalistische aannames over China. Het doen van onderzoek en het delen van kennis met het bedrijfsleven, NGOs en kennisinstituten zijn hierbij cruciaal. Dit moet leiden tot een strategie die enerzijds realistisch aanvaardt dat China zowel nationaal als op internationale toneel haar eigen koers zal varen, en anderzijds probeert China zo goed als mogelijk in te bedden in de internationale rechtsorde. Om dit mogelijk te maken is een uitbreiding nodig van de contacten tussen Nederland en China op officieel en onofficieel niveau. Tot slot is er een groeiend risico op onverwachte ontwikkelingen in cyberspace waarbij China een rol speelt. Het is wenselijk hier de nodige voorbereidingen voor te treffen.

Inleiding

In de Chinanotitie die recent is aangenomen in de Tweede Kamer,[1] spelen vraagstukken rond digitale technologie een belangrijke rol, verspreid over verschillende bedrijfsgebieden. Bijvoorbeeld spelen rond Huawei zowel handels- als veiligheidskwesties. De rol van digitale technologie in acties gericht tegen Oeigoeren in de regio Xinjiang, en de steeds toenemende controle van internetinhoud raakt rechtstreeks aan de fundamentele vrijheden die de kern vormen van het Nederlandse buitenlandse beleid. De risico's rond economische cyberspionage en mogelijke beïnvloedingsactiviteiten gericht op Nederlandse ingezetenen, contrasteren met de noodzaak tot samenwerking rond databescherming, technische standaardisering, en in het tegengaan van aanvallen zoals Mirai. Deze complexiteit wordt nog vergroot door het feit dat China zelf van technologie een absolute beleidsprioriteit heeft gemaakt, en dat technologie een centrale factor is in het voortdurende handelsconflict met de Verenigde Staten.[2]

Wat is dan de impact van het Chinese technologiebeleid op Nederlandse en Europese belangen, en hoe dienen Den Haag en Brussel hiermee om te gaan, op basis van de principes beschreven in de Chinanotitie? Met andere woorden, waar kan er worden samengewerkt, waar moet er worden beschermd? Dit rapport draagt bij aan een antwoord op deze vragen door (1) een kort overzicht te bieden van de grondslagen en kernelementen van het Chinese technologiebeleid, en (2) de raakpunten met Nederlandse belangen te inventariseren. Tot slot bevat dit rapport een aantal aanbevelingen, zowel richting het beleid omtrent China specifiek, als breder Nederlands technologiebeleid.

Een cybergrootmacht: China's technologische ambitie

Cybersecurity en informatisering

Hoewel wetenschap en technologie een centrale plaats innamen in het hervormingsbeleid sinds 1978,[3] betekende China's grote technologische achterstand dat het land tot voor kort grotendeels een volgende en, op het internationale vlak, passieve houding aannam. Dit is echter in het laatste decennium veranderd, omwille van een aantal factoren. Steeds beter wordende technologie kwam in steeds meer handen terecht, waardoor de maatschappelijke, politieke en economische rol van het internet snel toenam. De groei van China's eigen technologische ca-

[1] Ministerie van Buitenlandse Zaken. (2019). *Nederland-China: een nieuwe balans*. Netherlands

[2] Gros, D. (2019). This is not a trade war, it is a struggle for technological and geo-strategic dominance. *Cesifo Focus*, *20*(1), 21-26.

[3] Feigenbaum, E. (2003). *China's Techno Warriors*. Palo Alto: Stanford University Press.

paciteit, en protectionistisch beleid, stimuleerde de groei van eigen technologiebedrijven, voor online diensten, software en hardware. De Chinese regering ging technologie hoe langer hoe meer zien als een nieuwe economische groeipool, maar ook als onontbeerlijke component van goed en effectief binnenlands bestuur. Tegelijkertijd leidden zowel binnenlandse als buitenlandse incidenten tot groeiende zorgelijkheid over de mogelijke negatieve impact van technologie, bijvoorbeeld bij protesten en terrorisme, maar ook de kwetsbaarheid veroorzaakt door technologische afhankelijkheid van de Verenigde Staten.[4]

In februari 2014 kondigde president Xi Jinping derhalve aan dat een "cybergrootmacht" (*wangluo qiangguo)* worden, een nieuw doel van China zou zijn. Ter ondersteuning hiervan werd een nieuw coördinatieorgaan opgericht, de Centrale Leidinggevende groep voor Cybersecurity en Informatisering[5] (in 2018 hernoemd tot Centrale Commissie voor Cybersecurity en Informatisering – CCCI). Dit orgaan wordt voorgezeten door Xi Jinping persoonlijk, en verenigt alle senior beleidsmakers op ministerieel niveau binnen relevante staats- en partijorganen (inclusief de strijdkrachten). Daarnaast namen de bevoegdheden van de Cyberspace Administration of China (CAC), die o.a. de dagelijkse administratie van de CCCI uitvoert, stelselmatig toe.

Inhoudelijk, zoals de naam van de Commissie al aanduidt, steunt het beleid op twee poten: cybersecurity en informatisering. Deze worden gezien als een geïntegreerd en onlosmakelijk geheel, of in de woorden van Xi Jinping, "twee vleugels aan hetzelfde lichaam, twee wielen aan dezelfde wagen".[6] De definitie van cybersecurity is breed: waar deze in Westerse landen vaak beperkt blijft tot technische elementen, legt Chinees beleid de voornaamste klemtoon op de risico's die de inhoud van online informatie met zich meebrengt in een politieke, economische en maatschappelijke context.[7] In dat verband is ook de betrouwbaarheid van de onderliggende technologische systemen belangrijk, zodat ook de controle van, en beveiliging tegen, buitenlandse inmenging van informatiestromen zelf mogelijk is. Het cybersecurityregime zoals dit tot stand is gekomen onder de Cybersecuritywet van 2018,[8] richt zich derhalve op de beveiliging van persoonlijke en nationale veiligheidsgerelateerde data, een hiërarchische categorisering van in-

[4] Creemers, R. (2015). The Pivot in Chinese Cybergovernance. Integrating Internet Control in Xi Jinping's China. *China Perspectives*, *2015*(4), 5-14.
[5] Creemers, R. (2014). Central Leading Group for Internet Security and Informatization Established [Blog].
[6] Creemers, R. (2015). Speech at the 2nd World Internet Conference Opening Ceremony [Blog].
[7] Creemers, R. (2016). National Cyberspace Security Strategy [Blog].
[8] Creemers, R., Triolo, P., Webster, G. (2018). Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]. [Blog]

formatienetwerken met bijbehorende veiligheidsvereisten, het vrijwaren van kritieke informatie-infrastructuur en een verdere aanscherping van controle van online processen.

Informatisering, aan de andere kant, betreft het positieve gebruik van informatietechnologie ter ondersteuning van de ontwikkelingsdoelstellingen van de Partijstaat.[9] Het economische belang is hier duidelijk: technologiebedrijven genereren binnenlandse intellectuele eigendomsrechten, staan China toe verder op de ontwikkelingsladder te klimmen, kunnen ook ingezet worden ter verbetering van traditionele industrieën (in het "Internet Plus" plan[10] en Made in China 2025[11]), en nemen internationaal een groeiend marktaandeel in beslag. In politieke termen gelooft de Partijleiding dat toepassingen zoals big data en kunstmatige intelligente meer middelen verschaffen tot efficiënt bestuur. Bijvoorbeeld onderhouden overheidsinstanties van hoog tot laag contact met de burger via (private) sociale mediaplatformen.

Militaire en strategische vraagstukken

Wat in grote mate losstaat van dit hoofdzakelijk civiel beleidsdomein zijn de militaire capaciteiten en doctrines van het Volksbevrijdingsleger (PLA). Onder Xi Jinping is een hervormingsronde gestart met als doel dit leger in staat te stellen regionale conflicten succesvol te kunnen aangaan, en dus te professionaliseren. Ook de cybercapaciteiten (die o.a. ook geïmpliceerd waren in verregaande economische spionage tegen Westerse bedrijven) zijn niet aan de dans ontsprongen: de oorspronkelijke departementen 3PLA en 4PLA, respectievelijk bevoegd voor SIGINT en elektronische oorlogsvoering, zijn geïntegreerd in de nieuwe Strategische Ondersteuningsmacht (SSF).[12] Er is echter nog maar weinig duidelijk over operationele slagkracht of doctrine. Wel belangrijk is het concept "civiel-militaire convergentie" (*junmin ronghe*). Onder deze vlag poogt het leiderschap de technologische verworvenheden en efficiëntie uit de civiele economie in te zetten bij de hervorming van de strijdkrachten.[13] Het hoofdcommando werkt hierin nauw samen met de CAC. Eén belangrijke factor hierin is de creatie van een militair-industrieel complex volgens het Amerikaanse model, een ander

[9] State Council. (2016). *13th Five-Year Plan" for National Informatization.*
[10] Creemers, R. (2015). State Council Guiding Opinions concerning Vigoroulsy Moving Forward the "Internet Plus" Plan. [Blog]
[11] Zenglein, M., & Holzmann, A. (2019). Evolving Made in China 2025. China's industrial policy in the quest for glob-al tech leadership. *MERICS Papers On China*, (8).
[12] Kania, E. & Costello, J. (2019). The Strategic Support Force and the Future of Chinese Information Operations. The Cyber Defense Review. 3(1). 105-122
[13] Kania, E. (2019). In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate. [Blog]

component is de snelle omvorming van nieuwe technologieën naar militaire toepassingen.

In de inlichtingenwereld is China vooral bekend voor de eerder genoemde economische spionage. Reeds jarenlang pogen Chinese inlichtingendiensten technologische informatie te verzamelen, zowel voor nationale veiligheidsdoeleinden als voor de ontwikkeling van het Chinese bedrijfsleven. Ook gevoelige bedrijfsinformatie is vaak het doelwit, met name in de aanloop naar een overname of grote transactie. Deze activiteit heeft echter wel aan belang ingeboet, met name na de deal tussen Xi Jinping en Barack Obama in 2015.[14] Daarnaast richten Chinese activiteiten zich hoofdzakelijk op haar binnenlandse belangen. Een bijzonder gevoelig doelwit zijn de diasporische gemeenschappen in Europa, niet alleen van Han-Chinezen, maar met name van Oeigoeren en Tibetanen. Tevens lijkt China stelselmatig de cybercapaciteiten op te bouwen op inlichtingen- en beïnvloedingsvlak. Zo zouden Chinese diensten achter een hack van het Australische parlement en de grootste politieke partijen zitten,[15] en zou ook het interne e-mailverkeer van de EU gehackt zijn. Tot dusver zijn er in Europa echter nog maar weinig pogingen tot beïnvloeding door desinformatie gerapporteerd. Wel heeft een dergelijke campagne plaatsgevonden in Hong Kong.[16] Dit wordt door Beijing als grotendeels een interne aangelegenheid beschouwd, maar het gebruik van deze capaciteiten duidt aan dat Beijing ermee expertise opbouwt die mogelijk in de toekomst elders inzetbaar is.

Diplomatie en global governance

Op het internationale cybervlak heeft China tot dusver eerder een volgende rol gespeeld. Als deel van het bereiken van grootmacht status, wil Beijing echter ook haar "discoursmacht" (*huayuquan*) op het internationale vlak vergroten.[17] Daartoe organiseert de CAC jaarlijks de World Internet Conference, een show-event in het stadje Wuzhen, dat als platform dient voor de snelle ontwikkeling van de Chinese digitale industrie, alsook voor Chinese beleidsinitiatieven. Xi Jinping presenteerde er in 2015 de fundamentele elementen van China's internationale internetbeleid,[18] en in 2017 zou hier ook de internationale samenwerking rond de Digitale Zijderoute groots worden uitgerold.[19] Aangezien echter slechts een klein aantal landen deelnam, bleef dit

[14] Farley, R. (2018). Did the Obama-Xi Cyber Agreement Work? [Blog]
[15] Packham, C. (2019). Exclusive: Australia concluded China was behind hack on parliament, political parties – sources.
[16] Conger, K. (2019). Facebook and Twitter Say China Is Spreading Disinformation in Hong Kong.
[17] Creemers, R. (2016). Speech at the Work Conference for Cybersecurity and Informatization. [Blog]
[18] Creemers, R. (2015). Speech at the 2nd World Internet Conference Opening Ceremony [Blog].
[19] State Council Information Office. (2017). Initiative on Belt and Road digital economy cooperation launched.

initiatief relatief onbelicht. Daarnaast publiceerde het leiderschap ook een strategie voor internationale samenwerking in cyberspace, die – onder het mom van een "gemeenschap met een gedeelde lotsbestemming in cyberspace" (*wangluo kongjian mingyun gongtongti*), China's visie uiteenzet over welke principes en regels er dienen te heersen in cyberspace.[20]

Het belangrijkste principe hierin is soevereiniteit. Dit dient vooral in defensieve zin gezien te worden. De voornaamste internationale zorg in Beijing is dat de Verenigde Staten worden gezien als een existentiële dreiging: als een typische hegemoniale macht die de eigen leidende positie wil vasthouden, zal Washington niet aarzelen om de Partij pootje te lichten en de verdere groei van China te doen ontsporen. Het internet, en met name de open internet agenda die de Obama-administratie promootte, is in deze visie een Trojaans paard dat corrosie van het politieke systeem in de hand kan werken. Met het soevereiniteitsprincipe probeert Beijing dus te rechtvaardigen dat staten de exclusieve jurisdictie hebben binnen de eigen grenzen, en dus dat cyberspace wordt geterritorialiseerd. Ook wil Beijing daarmee aanduiden dat slechts staten de uiteindelijke beslissingsbevoegdheid hebben, de belangrijke rol van bedrijven, de technische gemeenschap en het maatschappelijk middenveld daargelaten.

Dit wantrouwen ten aanzien van de Verenigde Staten kleurt ook China's' houding in het lopende debat over normering van staatsgedrag. Beijing ziet het Amerikaanse standpunt over de toepassing van internationaal recht, inclusief humanitair en conflictrecht, als het voorbereiden van een juridische fundering die interventie in of agressie tegen China zal toelaten in de toekomst. Dit is ook een belangrijke bron van Chinese samenwerking met Rusland, een partner met wie een complexe en asymmetrische – doch op diplomatiek vaak innige – relatie bestaat.[21] De Chinese visie berust dus niet op een meningsverschil ten aanzien van bepaalde elementen van internationaal recht, maar een eerder globaal wantrouwen: internationaal recht is een middel voor machtige staten om hun positie te consolideren en concurrentie te vermijden. Daarom pleit China – hoewel het ook de eigen defensieve cyber capaciteiten uitbouwt – voor een demilitarisering van cyberspace.

Waar het gaat over Internet governance, heeft de eerdere Chinese onvrede met de structuur van het Internet Corporation for Assigned Names and Numbers (ICANN) plaatsgemaakt voor een mate van aanvaarding. ICANN's eerdere identiteit, als privaat bedrijf met een nauwe relatie met de Amerikaanse regering, deed velen in China vermoeden dat ICANN als wa-

[20] Creemers, R. (2017). International Strategy of Cooperation on Cyberspace. [Blog]

[21] Broeders, D., Adamson, L., & Creemers, R. (2019). A coalition of the unwilling? Chinese and Russian perspectives on cyberspace. *Policy Brief*.

pen tegen Chinese belangen zou kunnen worden gebruikt. Bijvoorbeeld zou het root server-systeem kunnen worden uitgeschakeld voor Chinees verkeer.[22] China pleitte er daarom voor ICANN onder te brengen bij de VN, of anderszins om te vormen tot intergouvernementele organisatie. Dit is niet gebeurd: de ICANN-transitie heeft geleid tot verzelfstandiging in een *multistakeholder* kader. Voor China was dit een aanzienlijke verbetering, en het ICANN-vraagstuk daalde in prioriteit. Echter blijven er bezorgdheden over de mate waarin Washington ICANN, dat nog steeds wettelijk een Amerikaans bedrijf is, zou kunnen verbieden diensten te verlenen aan China onder exportcontroleregels. Mede hierdoor blijft China vasthouden aan de houding dat ICANN "werkelijk onafhankelijk" dient te zijn van de controle van individuele staten, en een "multilateraal, democratisch en transparant" internet governance systeem nodig is.[23]

Wat wel snel een hogere prioriteit wordt, is de internationale stroom van data. De komst van de GDPR – die overigens in grote mate de ontwikkeling van Chinese regelgeving heeft beinvloed – heeft in Chinese kringen allerlei vragen losgemaakt over de noodzaak tot beveiliging van binnenlandse data, maar ook tot de mate waarin Chinese technologiebedrijven hoe langer hoe meer kwetsbaar zijn voor dataregelgeving in het buitenland. In binnenlandse regelgeving neigt de tendens steeds meer naar lokalisatie. Recente draft-regelgeving omtrent databescherming vereist zelfs dat binnenlands Internetverkeer binnenlands wordt gerouteerd.[24] Tegelijkertijd hoopt China op meer samenwerking ten aanzien van economisch dataverkeer, zowel wat betreft persoonlijke data als industriële data, met de Europese Unie. Hiermee poogt China reeds een basis te leggen voor de data-economie die met de uitbouw van 5G en het Internet of Things gepaard zal gaan.

Waar doorkruist het Chinese technologiebeleid Nederlandse belangen?

Uit dit verhaal kunnen een aantal principes worden afgeleid, die in beleid dienen te worden meegenomen:

- China's technologiebeleid heeft een breed draagvlak en een diepe historische basis, en zal niet worden stopgezet.

[22] Shen, Hong. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication*. 9(3). 304-324.

[23] N.a. (2019). China's Submission to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.

[24] Tai, K., Laskai, L, Creemers, R., Shi, M., Neville, K. and Triolo, P. (2019). Translation: China's New Draft 'Data Security Management Measures'. [Blog]

- Verscheidene Chinese doelstellingen en initiatieven zijn legitiem, de meesten zijn op zijn minst rationeel binnen de eigen logica.
- De relatie met de Verenigde Staten is het overkoepelende thema dat de Chinese houding ten aanzien van de buitenwereld bepaalt.
- China is geen monoliet: er zijn tegenstellingen binnen en tussen ministeries, alsook bedrijven, kennisinstellingen en professionele organisaties.

Uit bovenstaand overzicht blijkt ook dat de Chinese technologie-ambities zich uitstrekken over het gehele spectrum van politiek, economie en maatschappij. De raakpunten met Nederlandse belangen zijn derhalve talrijk en complex. Eén manier om deze in kaart te brengen is op basis van waar deze raakpunten zich manifesteren: binnen China, binnen Nederland, in derde landen, en op het internationale/diplomatieke niveau.

Binnen China

Zowel omwille van economische redenen als vanuit nationale veiligheidsoverwegingen heeft Beijing in de laatste jaren een omgeving gecreëerd waarin de eigen digitale "kampioenen" zichzelf konden ontwikkelen. Subsidies, beleidsondersteuning, beschermingsmaatregelen en technologieoverdracht behoren al langer tot de pijlenkoker van het Chinese beleid. Naarmate Chinese bedrijven steeds beter in staat zijn aan de binnenlandse vraag te voldoen, krijgen zij ook duidelijk voorrang op buitenlandse concurrenten in kritieke infrastructuur en overheidsnetwerken. Dit betekent dat de markttoegang voor Europese technologiebedrijven nog verder dreigt te verkleinen. Ook blijft de bescherming van intellectuele eigendom, hoewel er aanzienlijke vorderingen zijn geboekt in de laatste tien jaar, een punt van aandacht.[25]

Naast deze economische aspecten, zijn er ook strategisch-politieke elementen. De verregaande samenwerking tussen private spelers en de strijdkrachten in het civiel-militaire integratieprogramma doen vragen rijzen over de mogelijke mate waarin Europese *dual use*-technologie in de handen van de PLA zou kunnen vallen, alsook de mate waarin de resultaten van samenwerking tussen Nederlandse en Chinese universiteiten militair kan worden toegepast. Een tweede, voortdurende bron van zorg blijft de mensenrechtenkwestie. Het is duidelijk dat China niet binnen afzienbare tijd vrijheid van meningsuiting of organisatie zal dulden, en ook het recht op privacy is – tenminste waar het gaat over bescherming tegen de staat – niet afdoende gegarandeerd.[26]

Binnen Nederland

De steeds toenemende aanwezigheid van Chinese spelers in de Europese ruimte, doet zich in eerste instantie voelen door een groeiend marktaandeel van Chinese spelers in bepaalde sectoren. Deze markttoegang gaat niet noodzakelijk gepaard met evenwaardige en wederkerige behandeling van

[25] Nieuwe Balans: p. 27.
[26] Nieuwe Balans: p. 49.

Europese bedrijven in China. Daarnaast kunnen hier ook vragen gesteld worden over de Nederlandse en Europese strategische autonomie,[27] alsook het mogelijk risico dat kan worden gegenereerd door het gebruik van Chinese technologie. Dit kan zich op verschillende manieren manifesteren. Bijvoorbeeld, de vraag of Huawei-technologie aanwezig mag zijn in Nederlandse 5G-netwerken hangt niet alleen af van de mate waarin Huawei zelf als bedrijf betrouwbaar is, maar ook van politieke risico's. Enerzijds is het misschien mogelijk dat verdere Amerikaanse sancties het moeilijk maken om Huawei-componenten in de toekomst te updaten, upgraden en onderhouden, anderzijds kan een Chinees exportverbod ervoor zorgen dat deze componenten op korte termijn dienen te worden vervangen. Ook Chinese e-commercebedrijven, en met name Alibaba, zien hun marktaandeel toenemen in Nederland. Voor Nederlandse retailers betekent dit vaak het faciliteren van Chinese toeristen, bijvoorbeeld door betalingen via AliPay en TenPay mogelijk te maken. Het betekent echter ook toenemende druk op de Nederlandse logistieke sector, gezien geldende postverdragen betekenen dat zendingen vanuit China onder de kostprijs in Nederland dienen te worden geleverd. Verder zijn Chinese actoren actiever dan voorheen in het overnemen van Europese bedrijven, onder andere om technologie en knowhow te verwerven die in China nog niet aanwezig is. Zo werd de Britse chipontwerper Imagination overgenomen door een private equity firm gefinancierd door China.[28] Voor Nederland en Europa is het dus de vraag in welke mate deze investeringen dienen te worden tegengehouden, zowel om de export van mogelijk gevoelige technologie naar Beijing te beperken, als om de eigen strategische autonomie te behouden. Dit punt is ook belangrijk in de trans-Atlantische verhouding, getuige de recente beslissing van ASML om bepaalde apparatuur niet naar China te verschepen, op basis van Amerikaanse sancties.[29]

Wat betreft beïnvloeding door clandestiene cyber-kanalen, blijven Chinese operaties kleinschalig, maar groeit wel de gevoeligheid aan Nederlandse en Europese zijde.[30] In vergelijking met Rusland, bijvoorbeeld, is Chinese cyber-activiteit gering, en daar waar Russische operaties gericht zijn op disruptie van het publieke debat, is het Chinese doel eerder het genereren van een positieve publieke opinie over China en haar ontwikkeling. Het voortdurende maatschappelijke scepsis over China duidt aan dat deze missie tot op heden als onsuccesvol kan worden beschouwd. Desalniettemin komen er uit verschillende Europese landen, waaronder Zweden en Frank-

[27] European Commission. (2019). Rethinking Strategic Autonomy in the Digital Age. *EPSC Strategic Notes.* 30

[28] Kollewe, J. (2017). UK chip maker Imagination bought for £550m by China-backed tech firm.

[29] Cheng, T-F. and Li, L. (2019). Exclusive: ASML chip tool delivery to China delayed amid US ire.

[30] Nieuwe Balans, p. 51.

rijk,[31] waarschuwingen over spionage gericht op etnisch Chinese gemeenschappen, alsook daar verblijvende Tibetanen en Oeigoeren.

Derde landen

Nederlandse belangen zullen ook elders ter wereld meer en meer in contact komen met de groeiende Chinese technologische ambities.[32] Het belangrijkste voorbeeld hiervan is de Digitale Zijderoute (DZ), de digitale component van het Belt-Road Initiative (BRI). Net zoals de BRI is de DZ nog geen duidelijk omschreven en centraal georganiseerd beleidsproject. Vaak worden er eerder bestaande projecten in ondergebracht, of kleven Chinese bedrijven een DZ-label op standaard commerciële activiteiten die hoe dan ook zouden zijn ontplooid. *Grosso modo* kunnen de Chinese doelen als volgt worden gecategoriseerd. Ten eerste is dit een manier voor Beijing om een exportmarkt te creëren voor binnenlandse technologische producten, met lock-in effecten die ervoor zorgen dat ook volgende generaties technologie van dezelfde leverancier zullen komen. Ten tweede probeert China, door ervoor te zorgen dat meer landen een belang hebben bij het welzijn van de Chinese digitale sector, de internationale positie van de eigen bedrijven te bestendigen, met name waar het gaat over deelname aan internationale standaardisering, maar ook als verdediging tegen mogelijke sancties. In het bereiken van deze doelen geniet China een aantal aanzienlijke voordelen. Chinese bedrijven zijn, vanuit de eigen markt, vaak meer ervaren met het opereren binnen een minder ontwikkelde context, wat het makkelijker maakt de sprong te maken naar andere ontwikkelingslanden. Vanuit de ontvangende landen is het minder belangrijk dat de geïmporteerde technologie van absoluut topniveau is, zolang deze in eerste instantie voldoende functioneert. En Beijing stelt aanzienlijke financiële ondersteuning. Een derde belangrijke doelstelling van de DZ is geopolitiek: China hoopt op steun van ontvangende landen binnen internationale instituties zoals de VN, waar het debat over de toekomst van technologie volop woedt.

Internationaal/diplomatiek

Zoals eerder gesteld, is de houding van China binnen internationale gremia eerder defensief en reactief geweest. Hier komt stilaan verandering in, desalniettemin blijft China redelijk onervaren waar het gaat over global governance vraagstukken, en heeft het land een aantal onvermijdelijke strategische keuzes over haar plaats in de (cyber-)wereld vooruitgeschoven.

Het belangrijkste diplomatieke proces waarin Nederland en China elkaar in de multilaterale arena treffen, betreft de normering van staatsgedrag in cyberspace en het gebruik van informatietechnologie door statelijke actoren. Hier is China, samen met Rusland, de leider van een blok landen dat door het Westen soms als “coalition of the

[31] Garrus, J. (2018). No place to hide: exiled Chinese Uighur Muslims feel state’s long reach.
[32] Nieuwe Balans, p. 18.

unwilling" wordt benoemd. [33] Deze landen verenigen zich in een anti-Amerikaanse houding, waarbij soevereiniteit (en dus de eigen beslissingsbevoegdheid) voorop staat. Echter delen deze landen veel minder een positieve, constructieve agenda. Nederland positioneert zich in het kamp van de "like-minded states",[34] samen met andere Europese staten, de VS, Canada en Australië. Deze discussie bevindt zich echter, mede door deze tegenstelling, op dit moment in een impasse. De UN GGE-ronde van 2017 eindigde zonder consensus, en in 2018 stemde de Algemene Vergadering voor twee overlappende processen: een verlenging van de GGE en een Open-Ended Working Group (OEWG) on Information and Communication Technologies.[35] Of de aankomende rondes deze gremia uit impasse zullen komen, valt slechts af te wachten. Bij de eerste OEWG nam China een assertieve houding aan ten aanzien van het multistakeholder-karakter van dit proces, maar presenteerde ook een notitie over mogelijke beleidsopties die meer gedetailleerd was dan voorheen.[36] Een van de problemen is dat dit debat, alleszins in de Europees-Chinese context, niet gedragen wordt door bredere samenwerking, bijvoorbeeld via denktankkanalen of professionele dialogen. Zo is er bijvoorbeeld zeer weinig contact tussen Europa en China waar het gaat over militaire vraagstukken in cyberspace, en vinden bestaande track 1.5-initiatieven slechts sporadisch plaats. Dit limiteert ook de mogelijkheid om een basis te leggen voor vertrouwensopbouwende maatregelen.

Buiten VN-verband is de schaarste aan Nederlands/Europese interactie met China in het internationale veld niet in verhouding met het belang van de vragen die zich dienen te stellen. Hoewel technologie steeds meer wordt gezien als een veiligheidsaangelegenheid en minder een economische zaak, blijft het een feit dat de internationale handelsorde niet is toegerust om het hoofd te bieden aan de uitdagingen die de digitale economie stelt. Bijvoorbeeld het WTO-raamwerk over goederen en diensten dekt niet adequaat de nieuwe vormen van economische interactie die het internet mogelijk maakt. Met name rond dataverkeer ontstaat er een behoefte aan multilaterale oplossingen, daar waar de tendens nu vooral richting lokalisatie gaat.

---

[33] A coalition of the unwilling? Chinese and Russian perspectives on cyberspace.
[34] De Vries, H. (2017). Cyber in Nederland. [Presentatie]
[35] CCDCOE. (n.a.). A surprising turn of events: UN creates two working groups on cyberspace.
[36] China's Submission to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.

Aanbevelingen

Zoals dit korte overzicht aangeeft, beslaat de uitdaging die China's technologiebeleid aan de Nederlandse Chinastrategie stelt, een groot aantal beleidsvelden, en is deze vaak ingebed in bredere economische en strategische vraagstukken. Tot op zekere hoogte kunnen deze dus niet los worden gezien van de algemene stappen die Nederland dient te zetten op macroniveau.

- Het voornaamste antwoord op de vraag die China stelt, ligt binnen de eigen competentie, zoals ook al aangegeven binnen de Chinanotitie. Het is beter een duidelijke eigen strategische koers te kiezen en te varen, dan een reactieve opstelling aan te nemen. Hierin dient Nederland te investeren in de eigen concurrentiekracht, en een geïntegreerde aanpak uit te bouwen waarin effectieve coördinatie kan plaatsvinden tussen politieke, economische en maatschappelijke actoren.
- Ten aanzien van het veranderen van situaties in China moet realiteitszin voorop staan. De Nederlandse, en zelfs Europese invloed op Chinees binnenlands beleid is zeer beperkt. De nadruk dient dus te liggen op punten waarin (1) vooruitgang daadwerkelijk mogelijk is, (2) Nederland en Europa een zekere hefboom hebben en (3) kan worden gewerkt op basis van bestaande commitments aan Chinese zijde, of een duidelijke tendens richting convergentie.
- Geen enkele individuele Europese staat, en dus ook niet Nederland, wordt vanuit Beijing gezien als een evenwaardige partner. Het is slechts door samenwerken met EU-partners dat voldoende tegengewicht kan geboden worden aan de groeiende Chinese economische en politieke macht. Dit vereist ook dat er met lidstaten in Zuid- en Oost-Europa, die politiek dichter bij China staan, hierover een consensus wordt bereikt. Ook betekent dit gezamenlijk optreden op diplomatiek vlak, onder andere door nauwere samenwerking tussen de ambassades van de lidstaten en de EU-delegatie in Beijing.
- Hoewel de trans-Atlantische samenwerking van groot belang is en zal blijven in het Nederlandse veiligheidsbeleid, is het ook zaak om als Europa een zekere mate van autonomie te verwerven. In Beijing wordt Europa nog vaak gezien als een relatief onbelangrijke appendix van de VS. Het is dus zaak duidelijk te maken dat Europa een eigen koers vaart en een onafhankelijke, invloedrijke wereldspeler is.

Om een effectief engagement met China op cybervlak mogelijk te maken, zullen duidelijke keuzes en beslissingen moeten worden gemaakt. Deze zijn complex en zullen onvermijdelijk kosten met zich meebrengen, zowel economisch als in politiek kapitaal. Deze keuzes niet maken zou echter nog risicovoller zijn. Nederland dient

dus goed te overwegen wat haar inzet en prioriteiten zijn. Daarvoor is een kennis- en inzichtbasis nodig, die op basis van de volgende aanbevelingen tot stand kan worden gebracht.

- Op basis van het algemene overzicht dat de Chinanotitie biedt, is het nu tijd om over te gaan tot het detail. In eerste instantie vereist dit een inventarisering van de specifieke belangen die Nederlandse spelers, inclusief het bedrijfsleven en kennisinstellingen, hebben in en met China. Hiertoe dient de politiek nauwer te communiceren met het middenveld, o.a. door middel van koepelorganisaties (zoals FME voor de technologiesector, of VSNU voor hoger onderwijs).
- Het is ook nodig een inventarisatie op te maken van de beleidsgebieden en –vraagstukken waarin Nederland en China tegengestelde dan wel gelijklopende belangen hebben. Dit betekent dat een zerosum dynamiek beperkt kan worden tot gebieden waar dat zinvol is, terwijl op andere terreinen het gemeenschappelijk goed kan worden ondersteund.
- Binnen de diplomatieke context waarin samenwerking tussen Nederland en China niet alleen noodzakelijk, maar ook wenselijk is, is het nodig dat Nederland met haar partners het eens wordt over een *endgame* dat voor beide partijen aanvaardbaar kan zijn. Bijvoorbeeld in de discussie over normering van staatsgedrag is het wellicht onmogelijk dat de likeminded staten het gelijk volledig aan hun kant krijgen. Op welke punten die China voorstaat, kan er dus een compromis worden gevonden? Een secundair doel hier dient ook te zijn in welke mate China en Rusland enigszins uit elkaar kunnen worden gespeeld. De twee landen houden er een verschillende visie en operationele cultuur op na, waarbij China meer belang heeft bij een stabiele wereldorde.
- Tegelijkertijd worden er ook kansen gecreëerd door het feit dat China in deze internationale discussies nog redelijk onervaren is en ook kennis ontbeert. Hierdoor is het mogelijk voor Nederlandse en Europese stemmen om invloed uit te oefenen op nog steeds lopende beleidsprocessen in China. Bijvoorbeeld heeft China zich in grote mate geïnspireerd op de AVG in het opstellen van de eigen regelgeving omtrent databescherming. Hier is het met name nuttig om verder te spreken over concrete vraagstukken en maatregelen. Een verdere discussie over ver uit elkaar liggende principes zet geen zoden aan de dijk.
- Hiertoe is een aanzienlijke expansie nodig van het contact tussen de twee kanten. Er is natuurlijk een zekere gevoeligheid om dit te doen op het diplomatieke vlak, o.a. omwille van gerechtvaardigde zorgen dat dit Chinese processen en initiatieven (zoals de Wuzhen World Internet Conference) zou legitimeren. Dit kan deels worden ondervangen door het ondersteunen van dialogen gevoerd door

kennisinstellingen, economische koepelorganisaties en andere leden van het middenveld. Ook moet deze gevoeligheid vergeleken worden met het mogelijke nut van deze contacten. Niet alleen vormen deze een manier om meer kennis en inzicht over China te verwerven, zij zijn ook een kanaal om – in het geval van stijgende spanningen – het authentieke Nederlands/Europese standpunt te blijven communiceren aan ambtenaren die slechts zelden aan ongefilterde informatie worden blootgesteld.

- Tegelijkertijd is het ook belangrijk de eigen slagkracht op te bouwen om duidelijk paal en perk te stellen aan ongewenste vormen van Chinees gedrag. Zoals de Chinanotitie al aangeeft, is het niet wenselijk China ten allen koste te vriend te willen houden. Dit heeft een impact op economisch vlak, waar wederkerigheid en een gelijker speelveld van groot belang zijn. Het belang van de Europese markt voor Chinese bedrijven, met Huawei als bekendste voorbeeld, voorziet hier een mogelijk nuttige hefboom. Dit betekent ook dat het nodig is China-gerelateerde capaciteit op te bouwen binnen de veiligheids- en inlichtingendiensten, alsook binnen beleidsorganen. Het aantal Chineessprekende ambtenaren in deze diensten dient te worden vergroot, en efficiënter ingezet. Daarnaast kunnen verdere investeringen in attributiecapaciteit helpen bij het beknotten van het Chinese argument dat attributie onmogelijk is.
- Op de korte termijn is het mogelijk dat Nederland geconfronteerd zal worden met de gevolgen van Chinese cyber activiteit, bijvoorbeeld door spionage, mogelijke beïnvloeding, of – in het slechtste geval – pogingen tot intimidatie van in Nederland verblijvende dissidenten of leden van gevoelige etnische groepen. Het is wenselijk dat hiervoor vooraf scenario's klaarliggen, om een snelle en gepaste reactie mogelijk te maken.