Arnhem, 16 mei 2025

Als Stichting Internet Domeinregistratie Nederland (SIDN)[1] danken wij de vaste commissie voor Economische Zaken van de Tweede Kamer hartelijk voor de uitnodiging om aan een rondetafelgesprek over de Aanpak pakketstroom China deel te nemen – helaas zijn we verhinderd, echter we zijn de commissie erkentelijk voor de mogelijkheid inhoudelijk een bijdrage te kunnen leveren aan de discussie met dit position paper.

SIDN draagt zorg voor het beheer van het centrale register voor .nl domeinnamen, waarvan er meer dan zes miljoen zijn geregistreerd. Daarnaast ziet SIDN, verantwoordelijk voor de continuïteit en stabiliteit van het .nl domein[2], erop toe met een globaal gedistribueerde infrastructuur dat .nl domeinen wereldwijd ten alle tijden bereikbaar en beschikbaar zijn. Een doel van het gebruik van een domeinnaam is om via het Domain Name System (DNS) de vertaalslag te maken van een door mensen te herkennen (domein)naam naar een voor een computer te begrijpen numeriek Internet Protocol (IP) adres. Belangrijk om te beseffen is dat als register voor .nl domeinnamen SIDN geen enkele zeggenschap heeft over, dan wel inzage in, de (content op) websites waar de aan .nl domeinnamen gekoppelde IP-adressen naar verwijzen.

Als Internet infrastructuur aanbieder beschikt SIDN niet over expertise dan wel een expliciete opinie met betrekking tot het thema van het rondetafelgesprek, i.e. het 'Wat is er te doen aan de enorme instroom van producten uit China die niet voldoen aan de Nederlandse of Europese regels?'
In dit schrijven beperken we ons, samen met de Stichting Digitale Infrastructuur Nederland (DINL[3]), tot enkele eerdere vragen vanuit de commissie over het ontoegankelijk maken van online illegale content, het 'op zwart zetten' van 'websites' of 'platforms', wanneer 'onveilige of ongezonde producten' worden verkocht.[4]

SIDN veronderstelt dat het idee achter deze vragen is dat het 'op zwart zetten' ertoe zou moeten leiden dat Nederlandse gebruikers bepaalde websites niet -of minder makkelijk- kunnen bereiken, en vervolgens niet in de gelegenheid zijn daar door publieke autoriteiten als ongewenst beschouwde bestellingen te plaatsen.

Kernboodschap:
Samen met DINL bepleit SIDN dat het pogen om via de DNS af te dwingen dat websites 'op zwart' gezet worden, niet effectief is: het is makkelijk te omzeilen is en de bijbehorende onrechtmatige online content blijft beschikbaar. Bovendien heeft het potentieel schadelijke (ongewenste) nevengevolgen, en is het als principe in strijd met staand Nederlands overheidsbeleid dat ook internationaal uitgedragen wordt.

[1] https://www.sidn.nl/
[2] https://open.overheid.nl/documenten/ronl-2489709b0346453eb4bfa99cc0da2fd97c329bd3/pdf
[3] https://dinl.nl/
[4] https://www.tweedekamer.nl/kamerstukken/detail?id=2025D19466&did=2025D19466

Een ineffectief en schadelijk idee, het via het DNS websites 'op zwart zetten'

Domeinnamen blokkeren of deactiveren
In de context waarbinnen SIDN opereert, lezen we het 'op zwart zetten' van 'een website' of 'platforms' als het ingrijpen op domeinnamen, door middel van het aanpassen, manipuleren zo je wil, door tussenpersonen als ISPs van antwoorden op DNS verzoeken van eindgebruikers ('welk IP-adres hoort bij deze domeinnaam?'). Met het doel dat een gebruiker niet via de respons op een DNS verzoek bij een bepaalde, onrechtmatig geachte, website terechtkomt. Dit kan men DNS blocking of -filteren noemen. Een andere optie is het geheel deactiveren van de registratie van een domeinnaam, bijvoorbeeld een bij SIDN geregistreerd .nl domein, zodat deze nergens meer naar verwijst. En dus ook niet (meer) naar een als illegaal beschouwde website. Beide opties beschouwen we als niet effectief en bovendien als ongewenst want met schadelijke neveneffecten.

Principieel
De kracht van het Internet is dat het een wereldwijd systeem is, dat overal en voor iedereen op dezelfde manier werkt. Het internet is een open, gedecentraliseerd netwerk zonder centrale autoriteit die controle heeft over welke websites toegankelijk zijn. Dat betekent dat illegale online content primair moet worden bestreden bij de bron: door opsporing en vervolging van de aanbieders en het daadwerkelijk offline halen van hun aanbod door het voor eenieder onbeschikbaar te maken. Dat geldt voor alle onrechtmatige content, zoals misinformatie, CSAM, terroristische content en ook eventueel voor het online verkopen van 'onveilige of ongezonde producten'.

De werking van het Internet bestaat bij de gratie van het feit dat iedereen zich conformeert aan een gezamenlijke set protocollen en open standaarden die de kern van de internetinfrastructuur vormen. Gebruikers vertrouwen er indirect op dat het Internet conform deze protocollen werkt, dat ze daadwerkelijk online communiceren met de partijen waarmee ze dat wensen te doen - hoewel ze zelden of nooit over het onderliggende technisch functioneren van het Internet na zullen denken. Door ISP's op te leggen dat ze domeinnamen moeten blokkeren, grijp je in op één van de kernprotocollen van het internet, het eerdergenoemde DNS[5]. En daarmee breng je het neutraal en betrouwbaar functioneren van het Internet als technisch systeem in gevaar. Gaan we dit (als gevolg van precedentwerking) op steeds grotere schaal doen, dan wordt de huidige werking van, en daarmee het vertrouwen, in de werking van het Internet fundamenteel ondermijnd. Terwijl digitalisering voortschrijdt en de afhankelijkheid van online geleverde diensten steeds groter wordt. Dit zal niet alleen leiden tot aangepast gedrag van gebruikers om blokkades te omzeilen, wat technisch triviaal is door DNS instellingen in bijvoorbeeld de webbrowser aan te passen, en wat bevestigt dat de inzet van blokkades niet (structureel) effectief is. De content zelf is immers nog gewoon online beschikbaar. Ook kan het leiden tot het ontwikkelen en gebruik maken van andere methoden om te communiceren dan via het huidige DNS, waardoor we het risico lopen op fragmentatie van het Internet en het verlies van één van de pijlers van haar succes: een globale verbondenheid en interoperabiliteit, op basis van het vertrouwen in gezamenlijk gebruikte en niet gepolitiseerde open protocollen.

De Wetenschappelijke Raad voor het Regeringsbeleid wees er in 2014 al uitdrukkelijk op deze gevaren in haar rapport 'De publieke kern van het internet'[6]. De WRR concludeert daarin dat overheden uiterst terughoudend moeten zijn met beleid, wetgeving en operationele activiteiten die ingrijpen in de kernprotocollen van het internet waaronder het DNS. Bovendien zou non-interventie door overheden de internationale norm moeten zijn, daar waar het gaat om de kernprotocollen en de onderliggende technische infrastructuur van het wereldwijd verbonden publieke Internet. Het rapport adviseert de regering dan ook het beschermen van de publieke kern van het Internet een speerpunt te maken in haar diplomatieke inspanningen en wijst er daarbij terecht op dat 'practice what you preach' daarbij een minimumvereiste is. Oftewel, men kan niet aan de ene kant gidsland willen zijn en actief de bescherming van de publieke kern van het Internet uitdragen en dat ook vragen van anderen, en

[5] Een extensie op het DNS protocol, 'DNSSEC', moet er aan bijdragen dat een gebruiker kan vaststellen of de ontvangen DNS respons inderdaad technisch correct is, dat er niet van mogelijke manipulatie van het antwoord sprake is. Implementatie van DNSSEC wordt mede door het Forum Standaardisatie verplicht voorgeschreven voor publieke organisaties via de 'pas toe of leg uit' lijst https://www.forumstandaardisatie.nl/open-standaarden/verplicht

[6] https://www.wrr.nl/binaries/wrr/documenten/rapporten/2015/03/31/de-publieke-kern-van-het-internet/Synopsis-R94-publieke-kern-internet.pdf

anderzijds zelf doelbewust een inbreuk op die publieke kern maken door in Nederland ongewenste sites via het DNS te blokkeren. Los van het feit dat überhaupt niet echt effectief is.

Staand beleid met betrekking tot de publieke kern van het Internet
De vereiste bescherming van de publieke kern van het Internet, waaronder het DNS, en het actief internationaal uitdragen van deze boodschap en de verantwoordelijkheden die er mee samengaan, is inmiddels expliciet onderdeel geworden van de Nederlandse Internationale Cyberstrategie 2023-2028[7]. Ook de Nederlandse Strategie Digitale Economie[8], net als de daaropvolgende voortgangsrapportage, benadrukt het belang van de bescherming van de publieke kern voor wat betreft het functioneren van een niet gefragmenteerd, open, vrij en veilig Internet.

Gevaren
Het blokkeren van domeinnamen door ISP's is niet zonder gevaren voor derden. Een typefout wordt zo gemaakt (bijvoorbeeld uit gewoonte .nl achter een domeinnaam typen terwijl het om een .com gaat) met als gevolg dat de verkeerde domeinnaam niet meer bereikbaar is. Ook bestaat er een gevaar voor overblocking als bijvoorbeeld de site onder een sub domeinnaam chinesepakketten.provider.com gehost wordt en de hele domeinnaam wordt geblokkeerd waardoor andere -legale- sub domeinen onder provider.com ook niet meer bereikbaar zijn. Daarnaast moet de lijst van te blokkeren namen realtime en continu onderhouden worden, zowel door een bevoegde autoriteit als door de aanbieders die de blokkade moeten uitvoeren. Dat is een uitdaging op zich. En in de tussentijd blijft de gerelateerde content op websites of platforms gewoon beschikbaar, en is het omzetten naar een andere domeinnaam, alsook het via social media en search engines kenbaar maken van deze wijziging, triviaal.

Ineffectief
Door een ISP een domeinnaam te laten blokkeren, worden alleen de aangesloten klanten van die ISP beperkt in hun mogelijkheden om de website via die domeinnaam te bezoeken. De domeinnaam blijft voor de rest van de wereld actief, net als de website die daarmee kan worden bereikt. Zoals gezegd kan de website ook door de klanten van de blokkerende ISP zelf op andere manieren worden bereikt. Dit kan zowel door het actief gedrag van deze klanten, of met hulp van de illegale aanbieder of derden zonder dat de klant hier actief zelf iets hoeft te doen

Daarnaast zal blokkeren ineffectief zijn omdat het waarschijnlijk zal gaan om domeinnamen van websites die zich specifiek op Nederland richten. Veel van het in Nederland illegale aanbod zal in andere landen wel volkomen legaal zijn. Dit beperkt niemand om te bestellen bij het enorme aantal buitenlandse sites dat spullen naar Nederland levert en dat zich niet uitdrukkelijk op Nederland richt.

Deactiveren van een .nl domeinnaam?
Om dit moment heeft de Autoriteit Consument & Markt (ACM) de bevoegdheid, op basis van artikel 2.7 sub c van de Wet Handhaving Consumentenbescherming[9], om SIDN te vorderen een.nl domein te deactiveren. Hiermee kan de verwijzing naar een IP-adres bij een betreffende domeinnaam -al dan niet tijdelijk- verwijderd worden uit de .nl zone. Deze bevoegdheid is met voldoende waarborgen omkleed, en er is wat ons geen noodzaak voor additionele wettelijke bevoegdheden en/of -regelingen. SIDN hanteert daarnaast een door de industrie geformuleerde Notice and Takedown procedure[10] als het gaat om onmiskenbaar onrechtmatige content. Ook kan SIDN op basis van haar voorwaarden de registratiegegevens bij een domeinnaam verifieren[11]: als we het idee hebben dat een .nl-domeinnaam voor frauduleuze zaken gebruikt wordt, bijvoorbeeld omdat we daarop gewezen worden, dan starten we een onderzoek om de registratiegegevens te verifiëren. Als de houder niet binnen drie werkdagen aantoont dat de registratiegegevens correct zijn, dan kan SIDN de domeinnaam deactiveren, al dan niet tijdelijk. SIDN heeft overigens enkel technische zeggenschap over het beheer met betrekking tot .nl domeinnamen. Voor domeinnamen met andere extensies als .com moet men natuurlijk bij andere registers zijn.

[7] https://www.rijksoverheid.nl/documenten/publicaties/2023/06/09/internationale-cyberstrategie-2023-2028
[8] https://www.rijksoverheid.nl/documenten/rapporten/2022/11/18/rapport-strategie-digitale-economie
[9] https://wetten.overheid.nl/BWBR0020586/2025-03-01#Hoofdstuk2
[10] https://www.sidn.nl/nl-domeinnaam/klacht-over-inhoud-website
[11] https://www.sidn.nl/nl-domeinnaam/verificatie-registratiegegevens

Wat werkt wel?
Zorg voor een concurrerend legaal aanbod
Zoals gezegd valt het thema 'wat is er te doen aan de enorme instroom van producten uit China die niet voldoen aan de Nederlandse of Europese regels' buiten de deskundigheid van SIDN en DINL.

In algemene termen ligt het voor de hand om te zorgen voor een toegankelijk, concurrerend en aantrekkelijk legaal aanbod als alternatief voor ogenschijnlijk goedkope buitenlandse leveranciers. De gemiddelde Nederlander zal naar onze inschatting vanwege gemak, garantie, customer support, en op basis van een hoger vertrouwen sneller voor een dergelijk legaal aanbod kiezen dan naar illegaal aanbod uit te wijken waar onzekerheid over kwaliteit, levering, ondersteuning en retourbeleid een rol kunnen spelen.

Grijp in bij de bron
Mocht ingrijpen op online aanbod overwogen worden, dan dient men wat ons betreft naar de bron te gaan, dat wil zeggen daar waar, of door wie,de relevante content gehost wordt. En als het illegaal materiaal betreft, bij betreffende partij te vorderen dat die content verwijderd wordt.

De sinds februari 2024 van kracht zijnde Digital Services Act (DSA) vormt het centrale kader voor de bestrijding van illegale online inhoud in de EU, waarbij platforms verplicht worden risico's te beperken en transparantie te waarborgen. Op grond van artikel 9 DSA kunnen nationale autoriteiten of de Commissie zelf takedown-orders uitvaardigen, waarbij partijen wettelijk verplicht worden specifieke illegale content te verwijderen. De Europese Commissie benut deze wetgeving actief om onderzoeken in te stellen tegen Chinese online marktplaatsen zoals Temu en AliExpress, waarbij de focus ligt op de verkoop van niet-conforme producten, misleidende interface-ontwerpen en ontoereikende bescherming van consumenten. Ook hiervoor geldt het uitgangspunt dat illegale content bij de bron dient te worden aangepakt; bij het bedrijf dat illegale content host (of in dit geval illegale producten verkoopt). Als dat niet mogelijk is in het geval van in het buitenland gehoste websites, dan liggen in dit geval ingrepen in de fysieke pakketstroom wat effectiviteit betreft meer voor de hand dan ingrepen in de werking van het Internet.

We beseffen ons dat online leveranciers vaak vanuit jurisdicties opereren waar de Nederlandse autoriteiten niets te zeggen hebben, en waar Nederlandse verzoeken en vorderingen niet zullen worden opgevolgd. Daarom, en dat geldt eigenlijk voor alle zaken waarin het Internet een rol speelt, zal Nederland, net als alle andere landen, zwaarder moeten inzetten op internationale samenwerking. Dat het internet globaal is, is een gegeven, en alleen door samenwerking zal er effectief iets kunnen worden bereikt.

Conclusie
Het blokkeren alsook het deactiveren van domeinnamen heeft een beperkt beoogd effect. De content op gerelateerde sites blijft immers beschikbaar en het in te zetten blokkade instrument is makkelijk te omzeilen en een site is snel onder een andere domeinnaamextensie geregistreerd. Ingrijpen bij de bron om de rechtmatige content daadwerkelijk te verwijderen geniet ten alle tijden de voorkeur. Inzet van DNS blokkades brengt daarnaast risico's op fouten met zich mee, die ernstige consequenties voor derden kunnen hebben. Tot slot kan manipulatie van DNS gegevens, en/of de afhandeling van DNS verzoeken zonder dat de domeinnaamhouder daarom gevraagd heeft, de globale verbondenheid en interoperabiliteit, de eenheid, van het Internet in gevaar brengen. Terwijl het juist expliciet onderdeel van Nederlands beleid is dat we de publieke kern van het Internet willen beschermen en dat staten niet in deze kern interveniëren.

Bastiaan Goslings, namens SIDN
bastiaan.goslings@sidn.nl

Marijn van Vliet, namens DINL
mvanvliet@dinl.nl