

Hoever reikt de Amerikaanse macht op het internet? Kunnen de VS een landendomein, zoals .nl, zomaar uitzetten?

Marloes de Koning

Zestien jaar lang stopte Olaf Kolkman thuis twee keer per jaar een kleine goudkleurige sleutel in het mapje met zijn paspoort. Hij nam een vlucht van Schiphol naar Washington. Daar huurde de Nederlandse internetexpert een auto en reed de Amerikaanse hoofdstad uit, het platteland op.

Zijn bestemming lag anderhalf uur verderop, een datacenter in Culpeper, een stadje in de staat Virginia. Goed bereikbaar, maar ook net buiten het bereik van een potentiële nucleaire aanval op het Witte Huis of het Pentagon. „Om binnen te komen moest ik door vijf lagen beveiliging”, vertelt Kolkman, terwijl hij op zijn telefoon door foto’s bladert uit de tijd dat hij een van de veertien ‘sleutelhouders’ wereldwijd was, van 2006 tot en met 2022.

In het datacenter in Culpeper kwam hij uiteindelijk in een ruime cel met zwarte traliehekken en twee kluizen op ongeveer een meter van elkaar. Met de kleine goudkleurige sleutel opende Kolkman een kluislade. Hij haalde er een doorzichtig verzegeld zakje uit en hield het voor de lens van een camera. Zo kon iedereen zien dat het zakje nog dicht zat en dat dus niet met de inhoud – een smart card – was geknoeid.

Op de foto’s op zijn telefoon kijkt een handvol mannen in pakken toe en zet vinkjes op formulieren op clipboards. Ze hebben de rol van getuige, of van auditor, een ingehuurd controleur.

Het draaiboek met verschillende rollen en procedures telt 59 pagina’s. „Het is een hele poppenkast”, zegt Kolkman. Na een paar keer ging het behoorlijk vervelen. Maar het is belangrijk dat het gebeurt, zegt hij ook. In een datacenter in El Segundo in Californië aan de Amerikaanse westkust doorloopt een andere ploeg sleutelhouders twee keer per jaar hetzelfde procedé.

Met de smart card uit de eerste kluis activeerde Kolkman een cryptografische sleutel op een soort harde schijf in de kluis die ernaast stond. En om dié zwaarbeveiligde sleutel is het te doen. Want die cryptografische sleutel dient voor het ondertekenen van wat het best zou kunnen worden omschreven als het kadaster van het internet. Het systeem waarin wordt bijgehouden welk stukje internet van wie is.

Tot nu toe golden de VS als de machtigste verdediger van het vrije open internet en voelde het vanzelfsprekend dat alle kluizen daar staan

In deze analogie was Kolkman jarenlang een soort notaris die met zijn sleutel een watermerk zette op een voor het internet uitermate belangrijke database. Het is een soort adresboek vol verwijzingen, waardoor het dataverkeer op internet de weg kan vinden. Daarin worden namen zoals www.nrc.nl vertaald naar de adressen van computers op het internet.

De gewichtige ceremonie met de sleutels naar de ‘root server’, de wortel of stam van het internet, is nodig zodat computers wereldwijd zeker weten dat ze met het in Amerika beheerde origineel te maken hebben. En

niet met een kopie van dit wereldwijde adresboek. Want als daar twijfels over zijn of als er meerdere van dat soort adresboeken gaan circuleren, wordt het al snel chaos online. „Dan valt het internet uit elkaar”, zegt Kolkman. Dan heb je in plaats daarvan een ‘splinternet’, waarbij in verschillende delen van de wereld verschillende internetregels gelden en computers niet meer goed met elkaar kunnen praten.

Tot nu toe golden de Verenigde Staten als de machtigste verdediger van het vrije open internet en van democratische waarden in de wereld. En voelde het vanzelfsprekend dat alle kluizen daar staan. Maar dat verandert.

De hogepriesters die het internet besturen

Kolkman is inmiddels een veteraan in het internetbestuur. Hij heeft tal van verschillende functies gehad binnen internationale organisaties en bedrijven die zorgen dat het internet werkt en computers dezelfde technische taal spreken. Dat doet hij nog steeds, onder meer via overlegorganen over internetstandaarden en over digitale aangelegenheden bij de Verenigde Naties. De lange Nederlander omschrijft de ‘root key signing ceremony’ op een terras in de Randstad als een vorm van eervol vrijwilligerswerk binnen de internetgemeenschap. Na zestien jaar vond hij het wel genoeg en heeft hij het stokje overgedragen.

Als Kolkman erover vertelt, tekent hij er schema’s bij. Die laten zien: de wereld van het internet is anders georganiseerd dan die van de natiestaten. „Het hele systeem is gebaseerd op normatief gedrag. Niet op internationale wetgeving”, legt hij uit. Het is een onderwerp waarover hij ook gastcollege geeft aan de Vrije Universiteit in Amsterdam. „We proberen het met z’n allen zo te doen dat iedereen er baat bij heeft.”

De internetgemeenschap bestaat uit een complex web van samenwerkende stichtingen, bedrijven en adviesorganen van internationale organisaties die ervoor zorgen dat servers wereldwijd met elkaar kunnen communiceren. „Het werkt wonderbaarlijk goed”, concludeert Kolkman trots. Alleen al in Nederland wordt miljoenen keren per seconde succesvol het adres van een webpagina opgevraagd.

Dat onderliggende werk gebeurt grotendeels onzichtbaar voor gebruikers. Discussies over internet gaan meestal over de laag van de applicaties, de internettoepassingen die gebruikers zien. En dat gebrek aan aandacht vinden de mensen in de lagen daaronder wel prima.

Ze vormen een wereld op zichzelf die samen de wortels van het internet beheren. Het is een vrij informeel netwerk van „enorm onafhankelijke, libertaire mannen die het wel prima vinden dat niemand weet wie ze zijn en wat ze doen”, omschrijft Bert Hubert.

Hubert is in Nederland tegenwoordig vooral bekend als uitgesproken techduider op radio en tv. Maar hij is ook een van die mannen. Hij verdiende zijn sporen in de internetwereld met zijn softwarebedrijf PowerDNS. DNS staat voor Domein Naam Systeem en is het adresboek of kadaster voor het internet, waarover het in dit verhaal gaat.

Hubert is met zijn publieke profiel een uitzondering, want de meeste techneuten doen (in de woorden van Hubert) „het liefst alsof ze zelf een lijst nummers zijn, zonder politieke mening”. En dat geldt des te meer voor wat hij omschrijft als „de hogepriesters van het internet”, ook vaak „de mannen met de grijze baarden”

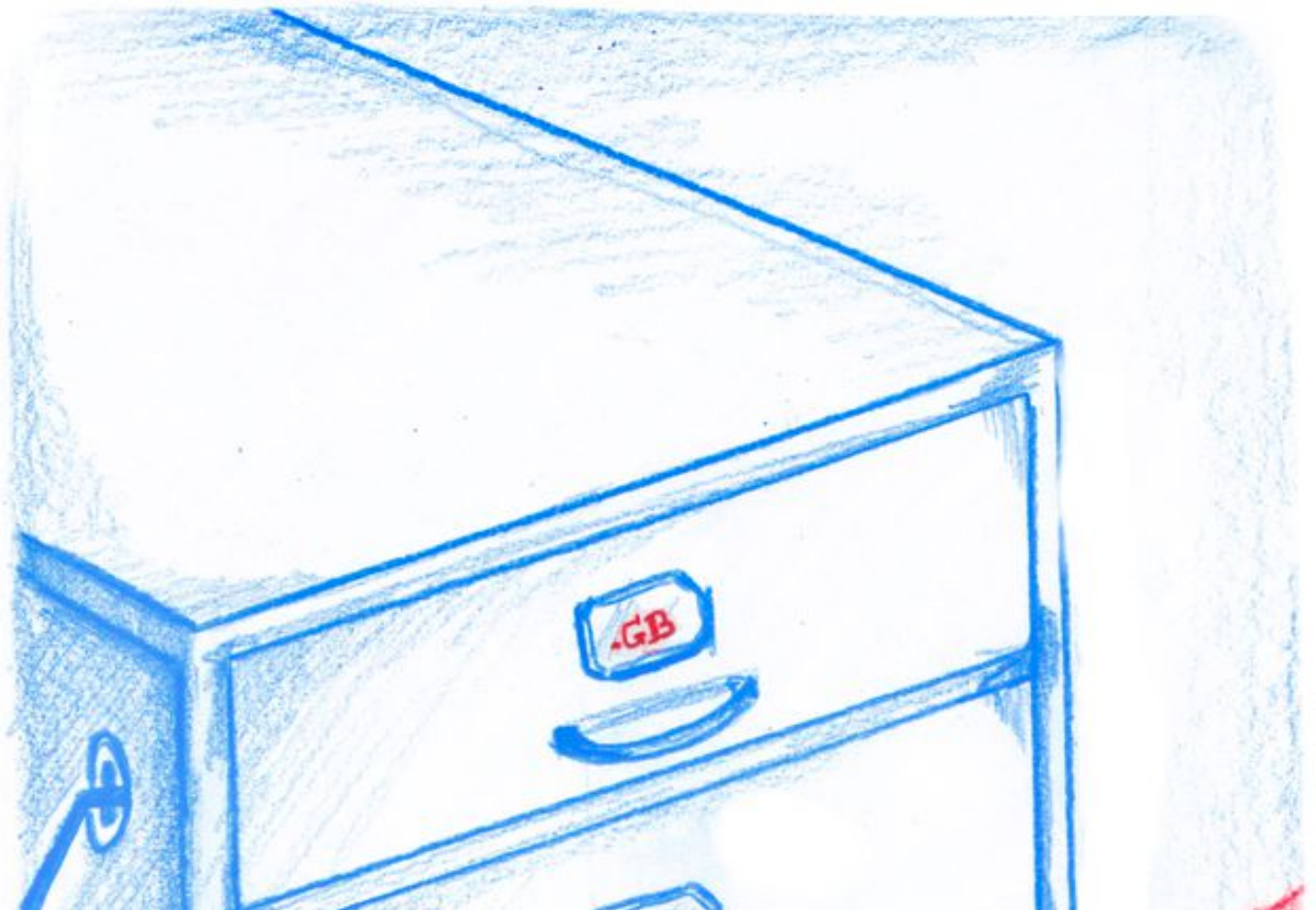
genoemd. „Die leveren best een topklus in het ontkoppelen van het internet van de politieke waan van de dag.”

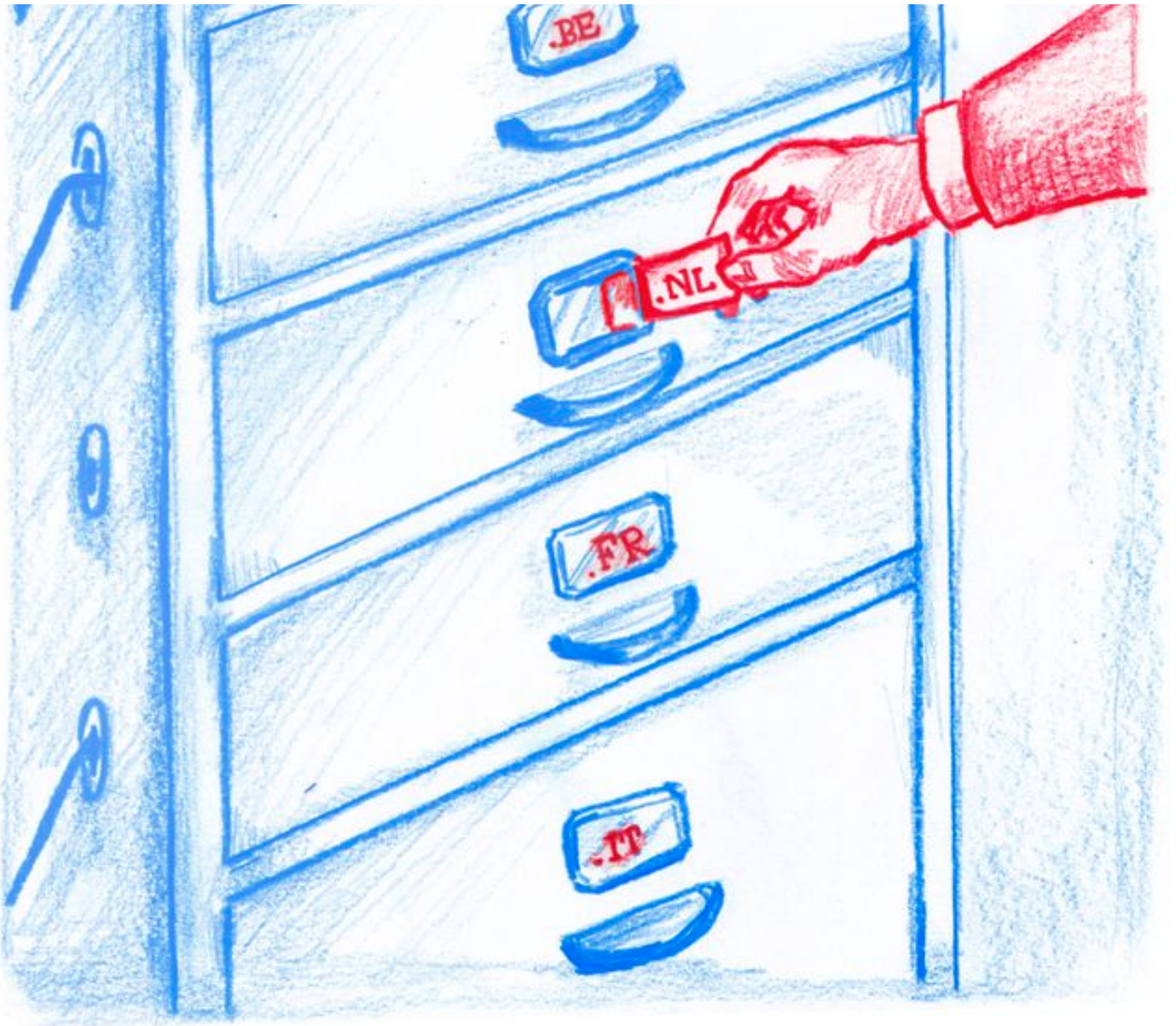
Die hogepriesters hebben een geloof. Namelijk dat het open vrije internet uiteindelijk goed is voor de mensheid. En dat transparantie en open communicatie democratie bevorderen. Als politici zich gaan bemoeien met het vrije verkeer van data komt dat al snel neer op censuur. Op autoriteiten die beslissen wie toegang heeft tot bepaalde informatie, of die mag publiceren.

Dé manier om het internet zoveel mogelijk vrij te houden van (geo)politiek is door de organisatie ervan decentraal te houden. Want je spreidt risico's als je ervoor zorgt dat er niet één punt is waarop je een verbinding kunt doorknippen. Wie de baas is over dat punt heeft immers de macht.

Maar dat is niet overal gelukt. Machtige organisaties voor het beheer van de domeinnamen voor de hele wereld, met namen als ICANN, IANA, PIR en Verisign, zitten allemaal in Amerika. Dat is tijdens de afgelopen veertig jaar (waarin het internet groot werd) zo gegroeid.

Want Amerika was wereldwijd de belangrijkste belangenbehartiger van het vrije open internet en verdediger van de vrijheid van meningsuiting. Steeds als er een poging was om iets te veranderen, bijvoorbeeld door de Verenigde Naties een rol te geven in de administratie van het internetadresboek, rolde de bal toch weer naar Amerika, dat met zijn techindustrie ook grote commerciële belangen heeft bij goed functionerende verbindingen. Liever een stichting in Amerika dan een VN-orgaan dat een speelbal is van onder meer China en Rusland, was steeds de conclusie als de discussie opspeelde. „Waar wilde je het anders doen”, vraagt Olaf Kolkman retorisch. Hij heeft ook een baardje.





Illustratie Leila Hak

Steeds diepere censuur

Maar wat als de belangen van Europese landen en die van de Amerikaanse regering niet helemaal dezelfde zijn? En de Amerikaanse regering terrorisemesancties uitvaardigt tegen bijvoorbeeld het Internationaal Strafhof in Den Haag, of tegen een Europese internetdienstverlener?

De afgelopen tijd verschenen verschillende amper opgemerkte rapporten over hoe de diepere lagen van het internet, zoals die van de domeinnamenadministratie en de zoeklabels, dreigen te politiseren, en wat de gevaren daarvan zijn. Bijvoorbeeld een [studie voor het Europees Parlement](#) over ‘Splinternets en het hernieuwde debat over fragmentatie op internet’. En een [rapport van de internationale denktank Article 19](#) over misbruik van het Domein Naam Systeem. „Censuurtechnieken van regeringen gaan steeds vaker de diepere lagen van de internetstack in, met een potentieel vernietigend effect”, staat daarin.

De Trump-regering is aan het testen hoever ze kunnen gaan

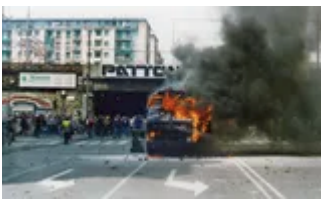
„De wereldwijde digitale infrastructuur is afhankelijk van de keuzes die de grote Amerikaanse techbedrijven

en de Amerikaanse overheid maken. Dat is nooit een prettige situatie geweest om in te zitten”, zegt Corinne Cath, directeur digitaal van Article 19. Ze is antropoloog en gepromoveerd op internetinfrastructuur. „En sinds Trump opnieuw aan de macht is ziet iedereen dit. Deze regering is aan het testen hoever ze kunnen gaan met die macht.”

Article 19 was een van de Europese ngo's die alarm sloegen toen de Amerikaanse regering op 26 augustus een Europese internetdienstverlener met de domeinnaam autistici.org op de sanctielijst plaatste, omdat die websites met extreem-linkse terreurboodschappen zou hosten. „Het is naïef om dat anders te zien dan een testcase”, zegt Cath.

[Lees ook](#)

[Als de Amerikaanse regering je tot terrorist heeft bestempeld: deze Italiaanse internetprovider kwam vorige week op de sanctielijst](#)



Als gevolg van die sanctie knipte de Amerikaanse organisatie die het beheer doet van de .org-domeinen (PIR) onmiddellijk de administratieve verbinding door en werd autistici.org onbereikbaar. Dat de internetdienstverlener in Italië zit en in Europa níét op terreurlijsten voorkomt, maakte geen verschil.

Het confronteerde spelers in de internetwereld met de macht van Amerika op hun domein. Maar hoever gaat die? Zou de Amerikaanse regering bijvoorbeeld hetzelfde kunnen doen met het hele ‘Punt-NL-domein’, dus alle websites die op .nl eindigen. Waarna Nederlanders opeens hun banken en overheden niet meer kunnen bereiken? En – in de woorden van Bert Hubert – „niets meer werkt wat op .nl eindigt. Kom dan bijvoorbeeld je parkeergarage nog maar eens uit.”

Op dat soort vragen geven de technische mannen uit de internetwereld het liefst technische antwoorden. Dan vertellen ze eerst over wat allemaal wél decentraal is: de kabels die overal ter wereld liggen. De datacenters die in alle landen staan. De overlegstructuren. De manier waarop wereldwijd naar consensus wordt gezocht over technische protocollen die vervolgens iedereen gebruikt.

Maar uiteindelijk zeggen ze ‘ja’ op de vraag of de Amerikaanse regering ervoor zou kunnen zorgen dat de .nl-domeinen onvindbaar zijn voor de rest van de wereld. Bijvoorbeeld met een presidentieel bevel of een sanctie.

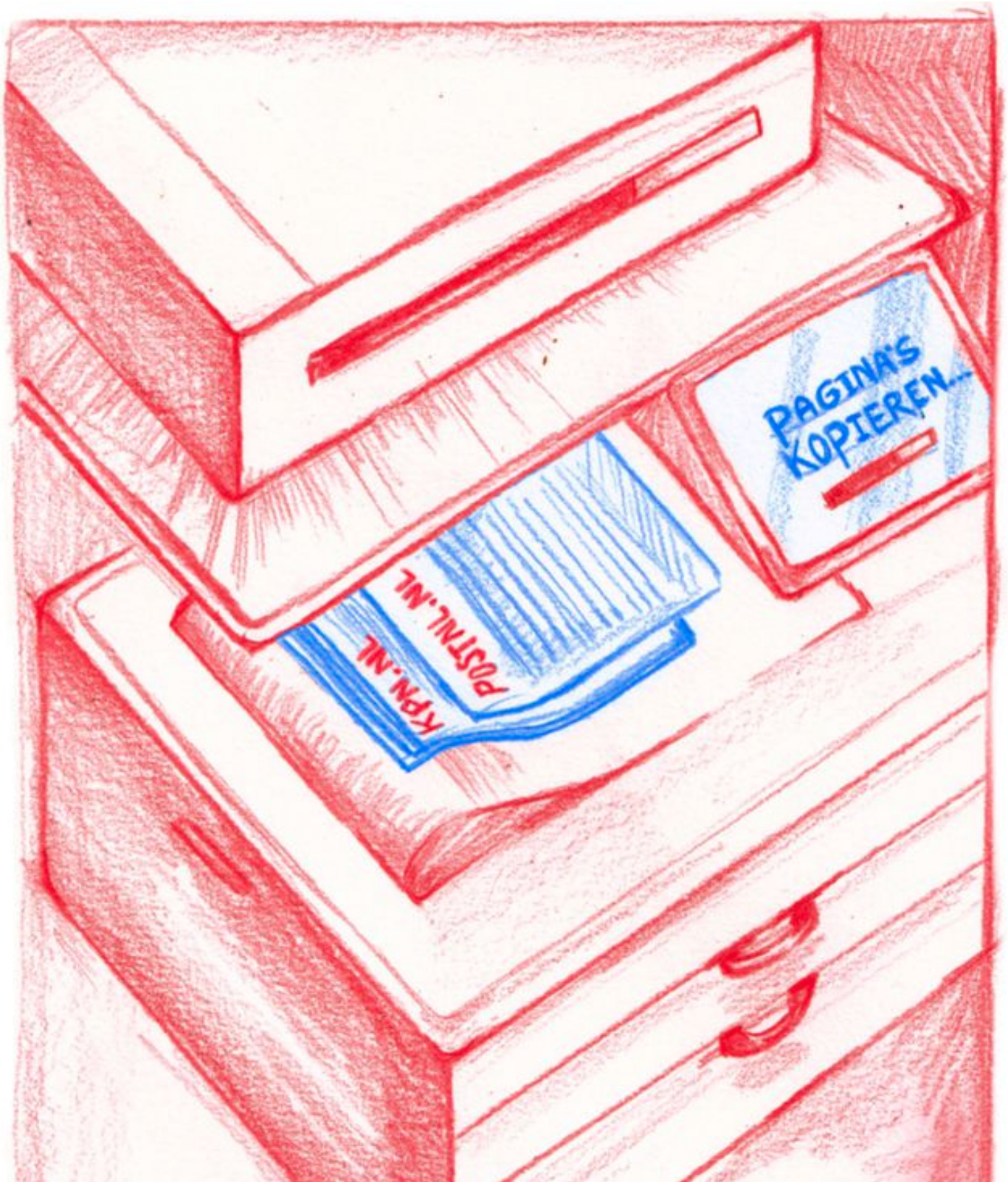
„Ja, dat kan”, zegt Hans Petter Holen. De Noor is ceo van RIPE NCC. Dat is de organisatie die (vanuit Amsterdam) het internetkadaster bijhoudt voor de regio waarin Europa, het Midden-Oosten en Rusland vallen. Hij heeft daardoor veel ervaring met sancties. Holen kijkt niet vrolijk als het over geopolitiek gaat. „Ik had nooit gedacht dat ik dat zou zeggen.”

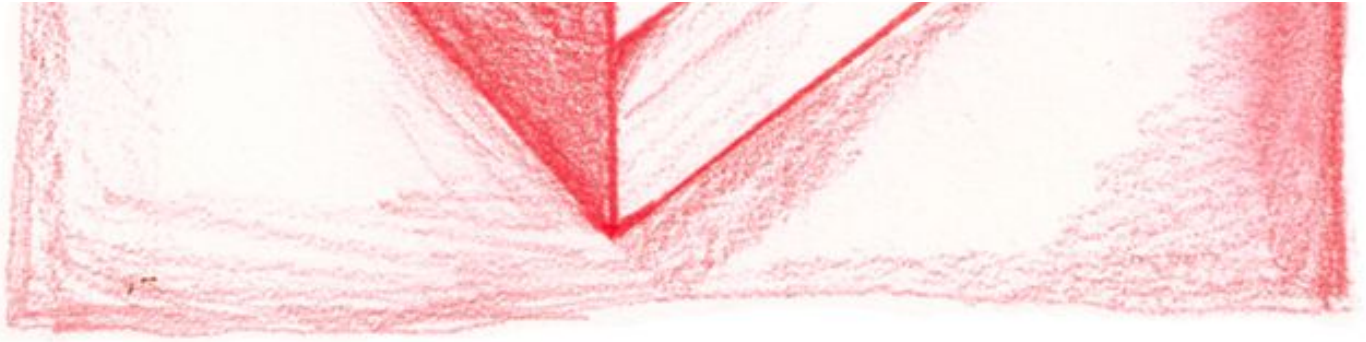
Ja, zegt ook tech-expert Bert Hubert. „De Amerikaanse regering hoeft alleen maar opdracht te geven.”

„Het kán wel”, zegt ook Olaf Kolkman na een korte stilte. Middels een sanctie tegen heel Nederland

waardoor Amerikaanse spelers in het domeinbeheer moeten gehoorzamen, omdat ze anders zelf vervolgd kunnen worden. „Maar het gebeurt niet.” De enorme Amerikaanse commerciële belangen bij het wereldwijde internet zijn in zijn ogen de belangrijkste garantie. Amerikaanse techbedrijven hebben razendsnel kunnen groeien doordat het internet zorgt voor één grote wereldwijde markt. Die willen niet dat het fragmenteert in verschillende werelddelen of dat landen worden geschrapt. „Het is te duur voor Amerikanen om het kapot te maken. Om het vertrouwen te verliezen. Daarmee zouden ze hun hele industrie onderuit halen.”

Maar zeker is hij er niet van.





Illustratie Leila Hak

Hoe zou dat werken?

Om te begrijpen hoe dat zou kunnen gaan, is wat uitleg nodig.

Internet is opgebouwd uit lagen. Er is bijvoorbeeld de laag van de technische afspraken, die protocollen worden genoemd. Gespecialiseerde mensen wereldwijd beslissen via een ingenieus consensusmechanisme mee over die protocollen, die vervolgens mondiaal gelden en waar iedereen van profiteert. Doordat die dezelfde ‘computertaal’ spreken, zijn webpagina’s wereldwijd op dezelfde manier te raadplegen.

Naast de techniek is er ook een administratief systeem, dat zich laat vergelijken met een telefoonboek of kadaster. Daardoor kunnen apparaten elkaar vinden aan de hand van hun IP-adressen. En dus zijn er ook administrateurs, die ervoor zorgen dat die administratie compleet en betrouwbaar is.

Ieder land heeft een eigen kadastertje, voor de websites met een landen-extensie. In Nederland is dat bijvoorbeeld de SIDN, Stichting Internet Domeinen Nederland. Maar het kadaster der internetkadasters wordt onderhouden in Amerika. Dat is de ‘root zone’ waarvoor Olaf Kolkman twee keer per jaar naar Amerika ging om middels de sleutelceremonie de authenticiteit te bekrachtigen. En daar is het internet een stuk minder decentraal.

De verdeling van de zogenoemde ‘top level’-domeinen – zoals van landen – is de verantwoordelijkheid van de Internet Corporation for Assigned Names and Numbers (ICANN). Het is een organisatie zonder winstoogmerk, die onder Californisch recht valt. Voor het wereldwijd organiseren van de domeinnamen heeft ICANN allerlei taken belegd bij stichtingen en bedrijven.

ICANN heeft de administratie van landendomeinen ondergebracht bij haar uitvoeringsorgaan IANA (Internet Assigned Numbers Authority), ook in een Amerikaanse entiteit. IANA organiseert de sleutelceremonies voor het watermerken van de ‘Root Zone Database’. En IANA doet de administratie van de .int-domeinen, die zijn gereserveerd voor internationale verdragsorganisaties, zoals het Internationaal Strafhof in Den Haag.

Het beheer van de .com-domeinnamen is een lucratieve aangelegenheid, die al jaren in handen is van het Amerikaanse bedrijf Verisign. Verisign doet dat ook voor onder meer .net en .cc en .name.

En alle domeinen die eindigen op .org, zoals die van veel stichtingen wereldwijd en van VN-organisaties, worden beheerd door de Amerikaanse stichting PIR.

Om te regelen dat een landendomein – zoals .de, .nl of .uk – niet meer werkt, kan de Amerikaanse regering opdracht geven aan ICANN, bijvoorbeeld via een presidentieel bevel of een sanctie. Amerikaanse personen, organisaties en bedrijven zijn verplicht dan te gehoorzamen. Als ICANN het betreffende ‘top level domain’ vervolgens schrapt uit het ‘internetkadaster’, is het voor computers en telefoons wereldwijd onvindbaar geworden.

Dat gaat geautomatiseerd en het is heel technisch: „Als ICANN een top level-domein zoals .nl uit de root zone verwijdt, wordt dat vervolgens geïmplementeerd door wat de ‘root zone signer’ wordt genoemd, dat is het Amerikaanse bedrijf Verisign”, legt Hans Petter Holen uit. „Vervolgens wordt het automatisch gedistribueerd over de hele wereld via de dertien verschillende root server operators, waar RIPE NCC er een van is.” RIPE NCC is in Nederland gevestigd en Holen is de ceo.

Er is ook een root server operator in Zweden en een in Japan. De overige tien zijn in de Verenigde Staten gevestigd. „De root zone is digitaal ondertekend. Als ICANN iets verwijdt uit het rootzonefile”, zoals .nl, „zullen wij door die ondertekening automatisch ook die update verspreiden. Dat kan ik niet aanpassen”, zegt Holen. „Het zou in mijn ogen wel ver buiten hun mandaat zijn als ze dat deden.”

Splinternet

Bij gesprekken over dit onderwerp komt er onvermijdelijk een moment waarop iemand over Rusland begint.

Na de Russische inval in Oekraïne in februari 2022 verzocht de Oekraïense regering aan ICANN en RIPE NCC om de door Rusland gebruikte top level-domeinen, waaronder .ru, te schrappen. ICANN en RIPE NCC weigerden dat te doen.

In de periode daarna zijn in Rusland voorbereidingen gestart voor het moment dat ICANN en RIPE NCC dat wél zouden doen en bijvoorbeeld de Amerikaanse overheid degene zou zijn die ICANN daartoe zou bevelen.

Die voorbereidingen komen erop neer dat alle Russische internetproviders op dat moment kunnen overschakelen op een kopie van de wereldwijde domeinnamenregistratie. Ze gebruiken dan niet langer het in Amerika met de sleutelceremonie gewatermerkte kadaster, maar een versie waarin de domeinen die op .ru eindigen nog wel bestaan.

In de rest van de internetwereld bestaat .ru dan niet meer. Maar in Rusland nog wel. Waardoor belangrijke functies, zoals internetbankieren of contact van burgers met hun overheid, door kunnen draaien.

De Russische voorbereidingen zijn in het Westen geïnterpreteerd als een teken dat Rusland zich zou willen afsplitsen, vertelt Hans Petter Holen. Een stap richting het gevreesde ‘splinternet’, waarbij het wereldwijde web niet langer wereldwijd zou zijn. Maar dat is niet hoe de Russen die hij spreekt dat zien. „Het is voorbereiding van de Russische overheid, voor het geval ze van buitenaf ontkoppeld worden.”

Bert Hubert vindt het door de toegenomen geopolitieke instabiliteit en de onvoorspelbaarheid van de Amerikaanse regering hoog tijd dat Europese internetproviders zo’n scenario ook eens oefenen. „De KPN’s en Ziggo’s van Europa kunnen zich voorbereiden en onderling bespreken onder welke omstandigheden ze het Amerikaanse internetkadaster niet meer volgen. Dat moet je voorbereiden en oefenen, anders verknaal je

het.”

Daar zou een krachtig signaal van uitgaan, denkt hij. „Daarmee verklein je gelijk de kans dat je het ooit echt zult moeten gebruiken.”

Ook Olaf Kolkman ziet dat het „vertrouwen in het systeem erodeert.” Wat hem betreft is er nog geen kantelpunt bereikt, maar zorgen maakt hij zich wel. Aan het einde van een lang gesprek vol technische uitleg en pogingen zo min mogelijk politieke uitspraken te doen zegt hij haast terloops: „Ik heb er in de vrije uren wel over nagedacht.”

Hij heeft ideeën over een technische benadering waarbij belanghebbenden het Domein Naam Systeem zouden kunnen blijven gebruiken tijdens een rampscenario. Dat vergroot de weerbaarheid. Dus om bijvoorbeeld .nl-domeinen in de lucht te kunnen houden terwijl de Amerikaanse regering ze wil schrappen? Kolkman: „Dat zijn jouw woorden. Maar ja, dat is zo’n onwaarschijnlijk rampscenario.”

Maak NRC jouw voorkeursbron op Google

Bij Google kan je nu zelf aangeven welke nieuwsbronnen jij vaker wil zien in je zoekresultaten. [Meer informatie](#)

[Kies NRC als voorkeursbron](#) Melding voorkeursbron sluiten