SPAMBESTRIJDING:

MANAGING A WICKED PROBLEM

KIRSTEN VERDEL

Spam spam spam spam. Lovely spam! Wonderful spam! Spam spa-a-a-a-a-am spam sp-a-a-a-am spam. Lovely spam! Lovely spam! Lovely spam! Lovely spam! Lovely spam! Spam spam spam spam!

(Zoals gezongen door een groep Vikingen in de beroemde Monty Python 'spam' sketch)
www.detritur.org/spam/skit.html

Spambestrijding: managing a wicked problem

De grenzeloze overheid?

Kirsten Verdel
Studentnummer 262654
Opleiding Bestuurskunde
Erasmus Universiteit Rotterdam
Begeleider: Prof. dr. Wim Derksen
Moulins-Engilbert, Frankrijk, november 2004
Eindbewerking Ottawa, Canada, april 2005
Faculteit der Sociale Wetenschappen

SPAMBESTRIJDING: MANAGING A WICKED PROBLEM

Doctoraalscriptie bestuurskunde

Erasmus Universiteit Rotterdam
Faculteit Sociale Wetenschappen

Voorwoord

Het afgelopen jaar was op zijn zachtst gezegd nogal turbulent. Als ik dit schrijf is het 29 oktober 2004 en ik zit op een zolderkamer in een oude boerderij in het Franse Moulins-Engilbert naar buiten te kijken. Ik heb uitzicht op zacht glooiende heuvels en de regen tikt clichématig tegen het raam. Ik begin zometeen aan de laatste vier hoofdstukken van mijn scriptie waar ik negen dagen de tijd voor heb. Dit voorwoord schrijven is mijn laatste uitstelgedrag voordat ik daaraan begin. Weemoed maakt zich op zo een moment meester van het denken. Het dwingt mij tot enige reflectie.

Als er iets is dat ik geleerd heb in de afgelopen 23 jaar waarin ik onderwijs heb mogen genieten, dan is het wel dat het er voor mij heel erg toe doet van wíe ik onderwijs mag genieten. Ik moet en wil geïnspireerd worden, wil ik zelf met volle overtuiging ergens voor gaan. Die inspiratie kreeg ik op de middelbare school onder andere van Gerard Schelvis, Yol van Breukelen en Jan van der Westen, die mij niet alleen steunden met onderwijskundige kennis, maar die ook mijn eeuwige helden zijn na alles wat er op het Bona gebeurd is en om wat zij daarna voor mij hebben gedaan. Het is inmiddels zeven jaar geleden dat ik mijn VWO-diploma haalde, maar het feit dat ik nu bij Jan thuis zit om dit verhaal te tikken zegt genoeg.

Na die fantastische jaren op het Bona was de opleiding journalistiek in Utrecht een strafkamp. Onpersoonlijk, saai, ambitieloos. Ik stopte en was gedurende twee jaar op zoek naar een nieuwe toekomst. Uiteindelijk besloot ik om bestuurskunde te gaan studeren met het voor mij heilige doel om die opleiding af te maken. Dat viel mij zwaar, want ook hier was de afstand groot, en de inspiratie mijnerzijds eufemistisch gesteld tamelijk gering.

Maar ruim een jaar na aanvang diende zich plotsklaps Wim Derksen aan. Ineens ging bestuurskunde ergens over, ineens kon ik dingen plaatsen, kreeg ik er echt zin in. Ik werd weer geïnspireerd. Ik leerde de faculteit beter kennen en maakte daar een aantal soms hele speciale vrienden. Gerbrand, Job, Daniel, Josta... merci beaucoup...

Ongeacht of de laatste vier hoofdstukken die ik moet gaan schrijven deze scriptie tot een goed einde brengen, ben ik allang blij met de situatie waar ik in verkeer. Ik heb niet alleen veel te danken aan Jan, Wim c.s., maar ook aan XS4ALL. Al die jaren dat ik daar gewoon 40 uur per week werkte kreeg ik alle tijd en ruimte om mijn studie te doorlopen. Uiteindelijk is daar één iemand wat mij betreft rechtstreeks voor verantwoordelijk: Doke Pelleboer. Ook jij ontzettend bedankt. En natuurlijk vergeet ik Pim niet. Zonder Pim hadden mijn scriptie en Word nooit vrede kunnen sluiten. Wilco muchas gracias voor de vormgeving!! Enne dinges... bla!

Het wordt tijd dat ik begin. Maar voordat ik dat doe, nog één keer die ene zin die mij dit jaar overal doorheen heeft gesleept: het is beter te streven naar het onmogelijke dan te berusten in het haalbare.[1]

Kirsten Verdel
Moulins-Engilbert, 29 oktober 2004

[1] Of zoals het beter (zijdelings) verwoord staat in de Hitchhiker's Guide to the Galaxy:
'The trick to flying is being able to throw yourself at the ground and miss.' Kwestie van oefenen dus!

INHOUDSOPGAVE

Hoofdstuk 2

Hoofdstuk 3

Hoofdstuk 4

Hoofdstuk 5

Hoofdstuk 6

Hoofdstuk 7

Inhoudsopgave bijlagen

Lijst van afkortingen

ADSL	Asymmetric Digital Subscriber Line
BCC	Blind Carbon Copy
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CC	Carbon Copy
DNS	Domain Name Server
DOS	Denial of Service
E-MAIL	Electronic Mail
EU	Europese Unie
FAQ	Frequently Asked Questions
HTML	Hyper-Text Markup Language
ICT	Informatie- en Communicatie Technologie
ID	Identification Code
IP	Internet Protocol
ISP	Internet Service Provider
IViR	Instituut voor Informatierecht

Lijst van afkortingen - vervolg

MFA	Mail Filter Agent
MIME	Multi-purpose Internet Mail Extensions
MSA	Mail Storage Agent
MTA	Mail Transfer Agent
MUA	Mail User Agent
NLIP	Nederlandse Internet Providers
OECD	Organisatie voor Economische Samenwerking en Ontwikkeling
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
TACD	Transatlantic Consumer Dialogue
TCP	Transmission Control Protocol
UBE	Unsolicited Bulk E-mail
UCE	Unsolicited Commercial E-mail
VN	Verenigde Naties
VS	Verenigde Staten
WIPO	World Intellectual Property Organization
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Samenvatting

Spam (ongewenste e-mail) is een probleem. Uit diverse onderzoeken blijkt dat ongeveer de helft van alle e-mail uit spam bestaat. De sociale en economische kosten van spam zijn hoog, het belemmert de informatie uitwisseling op internet en het maakt inbreuk op de privacy van de ontvanger. De analyse van de vraag wat anno 2004 de problemen zijn met betrekking tot spambestrijding en hoe de (Nederlandse) overheid met spambestrijding omgaat staan centraal in deze scriptie. Met als uiteindelijke doel het doen van aanbevelingen om spambestrijding waar mogelijk effectiever te laten verlopen. De centrale vraagstelling van de scriptie is: ‘Kan de overheid een rol spelen met betrekking tot spambestrijding, en zo ja: voor welke overheid is welke rol weggelegd?’

Om spam te kunnen bestrijden is het noodzakelijk om te weten hoe e-mail precies werkt en hoe het technische proces achter spam precies in elkaar steekt. Spam blijkt door de ontvanger niet eenzijdig af te stoppen, want dankzij de technische onvolkomenheden van e-mail zijn spammers in staat om door middel van talloze technische trucs hun spam e-mails af te blijven leveren bij honderden miljoenen internetters. Daarnaast is het relatief eenvoudig om spam te versturen. Een computer en een internetaansluiting zijn voldoende om wagonladingen ongewenste e-mail te versturen.

Technische filters die internetgebruikers installeren om spam te weren volstaan niet, maar wet- en regelgeving die het versturen van spam verbiedt, is ook geen afdoende maatregel om spam te bestrijden. De spammer is namelijk in staat om zijn fysieke locatie (en daarmee zijn identiteit) te camoufleren door bijvoorbeeld het afzenderadres te vervalsen of door de spam door middel van gehackte pc's van andere gebruikers te versturen. Alleen als dit niet gebeurt of als de spammer zijn geld op gaat halen, is het mogelijk om hem te pakken te krijgen. Niet alleen het versturen van spam is eenvoudig, ook het ontwijken van eventuele blokkades of represailles is voor spammers vaak een fluitje van een cent. Hoe komt dat nu?

Spambestrijding blijkt ingewikkelder te zijn dan het installeren van een technisch filter en het simpelweg verbieden van spammen. De opvattingen over wat spam precies is lopen te ver uiteen bij de bij spambestrijding betrokken actoren. Zij hanteren allemaal verschillende percepties over de definitie van spam. De ontvanger van spam wil er niets mee te maken hebben, de verzender ziet het juist als zijn broodwinning. Internetproviders, consumenten(organisaties), bedrijfsleven en direct marketeers hanteren ieder een eigen definitie van spam. Om aan alle eisen van die actoren tegemoet te komen zou in de definitie van spam rekening gehouden moeten worden met commercieel gedrag, de psychologie van de ontvanger, de juridische context, economische overwegingen en technische belemmeringen en mogelijkheden. Het is bijna onmogelijk om een definitie te hanteren die al deze elementen bevat. In deze scriptie hanteer ik de definitie die er het dichtst in de buurt komt: ‘Spam is het (massaal) versturen van ongevraagde berichten op internet met dezelfde boodschap, meestal met een commerciële inhoud, maar soms ook met een wervende politieke of charitatieve boodschap.’

Spam veroorzaakt niet alleen problemen, maar is zelf ook het gevolg van een ander probleem. Door ICT-ontwikkelingen zijn begrippen als ‘afstand’ en ‘tijd’ een wezenlijke andere rol gaan spelen. Veel activiteiten kunnen dankzij ICT wereldwijd worden ontplooid, onafhankelijk van de geografische locatie. De afnemende binding aan een bepaald grondgebied (deterritorialisering) heeft ‘onvermijdelijke gevolgen voor het handelingsvermogen van de nationale staat’, door de gebondenheid van instrumenten aan territoriale grenzen. Zo is wet- en regelgeving onlosmakelijk aan territoir gebonden. Grensoverschrijdende activiteiten vereisen

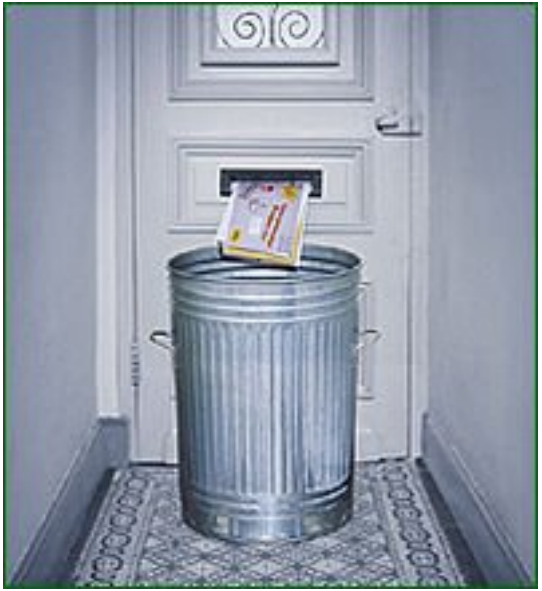
(wereldwijde) samenwerking in steeds horizontalere netwerken. De veranderende gezagsverhoudingen in deze netwerken leiden tot veelal uiterst complexe problemen (wicked problems), waarbij interactie met andere actoren noodzakelijk is om tot oplossingen te komen, doordat in netwerken wederzijdse afhankelijkheden zijn ontstaan.

Meer samenwerking lijkt in theorie dan ook een weg naar een oplossing te zijn. De maatregelen om spam te bestrijden zouden dan net als spam zelf grensoverschrijdend moeten zijn om effectief te kunnen zijn. Samenwerking tussen nationale staten lijkt onvermijdelijk om tot een oplossing van het spamprobleem te komen. De bij spambestrijding betrokken actoren moeten een gezamenlijk referentiekader ontwikkelen. Daar zijn een aantal voorwaarden aan verbonden. De actoren in het netwerk moeten zich er van bewust zijn dat ze van elkaar afhankelijk zijn bij het bereiken van hun doelen, ze moeten openstaan voor de belangen en percepties van andere actoren in het netwerk en ze moeten beseffen dat die andere actoren elk hun eigen achtergrond hebben. Door te streven naar gezamenlijke doelen, het creëren van variëteit om fixatie te voorkomen, het maken van procesafspraken in plaats van te discussiëren over de inhoud, het afspreken van duidelijke criteria, het aanstellen van een arbiter, het maken van afspraken over toe te laten actoren, het afspreken van een beloningsstructuur en het aanscherpen van de condities voor samenwerking kan dit bereikt worden. Een facilitator of *game manager* moet ervoor zorgen dat het proces op gang komt, op gang wordt gehouden en dat de samenwerking duurzaam is. Hij moet arena's aan elkaar koppelen, de agenda bijhouden, expertise regelen, knelpunten signaleren en voortdurend de gang van zaken evalueren. En om ervoor te zorgen dat de andere actoren hem accepteren, moet hij neutraal zijn, vertrouwen opwekken, gezag uitstralen en competent zijn. Tot zover de theorie, maar hoe werkt dit nu in de praktijk bij spambestrijding?

De samenwerking blijkt bij spambestrijding niet voldoende te zijn, hetgeen leidt tot de vraag: wat wordt er eigenlijk gedaan om spam te bestrijden? Er blijken verschillende methoden te zijn, met elk hun eigen onvolkomenheden. *Technische filters* filteren ook gewone e-mail of laten juist spam door, *economische maatregelen* blijken vooral erg onpraktisch te zijn en de voorwaarden voor dit soort maatregelen zijn niet aanwezig, *wet- en regelgeving* is nog volop in ontwikkeling maar staat net als *voorlichting* vrijwel overal nog in de

kinderschoenen en *zelfregulering* faalt omdat de meeste spammers juist crimineel zijn en zich niet zullen binden aan brancheorganisaties die zelfregulering op het oog hebben. Toch zijn dit de enige mogelijkheden die voorhanden zijn om het spamprobleem te bestrijden. Het vormen van een zo breed mogelijk front tegen spammers door een combinatie van al deze maatregelen lijkt de meest optimale oplossing van het spamprobleem te zijn. Samenwerking tussen de verschillende betrokken actoren om alle vormen van spambestrijding inhoudelijk op elkaar aan te laten sluiten is derhalve noodzakelijk, maar vooralsnog afwezig.

De volgende stap was dan ook het in kaart brengen wie nu precies de betrokken actoren zijn en wat hun belangen en percepties zijn. Wordt er in de verhoudingen en interactie tussen de betrokken actoren bij spambestrijding voldaan aan de voorwaarden die de netwerkbenadering stelt aan een succesvolle manier van het benaderen van een beleidsproces, of is de praktijk weerbarstiger? De belangrijkste actoren zijn overheden, zakelijke markt, consumenten, direct marketeers, internet service providers, de media en spammers zelf. De samenwerking tussen deze actoren blijkt nog niet voldoende van de grond te komen door een aantal factoren. Ten eerste zijn de onzekerheden over inhoud, instituties en strategie nog te groot. Ten tweede er is wel een gemeenschappelijk referentiekader (spam moet bestreden worden), maar binnen dat kader lopen de meningen nog te veel uiteen. Ten derde zijn er nauwelijks blokkades voor interactie en zelfs top-down sturing zou mogelijk zijn, maar er ontbreekt een instituut waarbinnen die interactie en sturing plaats kunnen vinden. Ten vierde is er geen sprake van bewuste of opzettelijke geslotenheid van actoren, maar de



meeste actoren handelen nog niet echt open. Hetgeen weer te maken heeft met het vijfde punt: het onvoldoende aanwezige besef dat de actoren bij spambestrijding wederzijds van elkaar afhankelijk zijn.

In de praktijk wordt er dus nog niet genoeg gedaan met de handvatten die de theorie biedt om tot oplossingen te komen voor complexe problemen zoals spambestrijding. Als men toch vooruit wil met spambestrijding dan zal er op een aantal punten steviger ingezet moeten worden. De vraag hoe spambestrijding dan wel beter zou kunnen gaan probeerde ik dan ook in het laatste hoofdstuk te beantwoorden.

Dat wet- en regelgeving juist datgene zijn wat nog in grote mate ontbreekt in de aanpak van spambestrijding, gecombineerd met het feit dat de betrokken actoren allemaal naar ‘de overheid’ wijzen als de centrale actor (!) die sturing moet geven bij de aanpak van spam, leidde tot het zoeken naar een supranationale organisatie die bevoegd zou zijn om grensoverschrijdende maatregelen te nemen tegen spam. Dit moet wel een overheidsvorm zijn, daar andere actoren niet democratisch gelegitimeerd zijn om wet- en regelgeving vast te stellen. De Verenigde Naties is dan een voorbeeld van het type organisatie dat nodig is om spam effectief te kunnen bestrijden. De VN zou door middel van het VN-onderdeel WIPO als facilitator op het gebied van spambestrijding kunnen optreden. De WIPO kan een neutrale positie innemen en tegelijkertijd een platform bieden voor de totstandkoming van grensoverschrijdende wet- en regelgeving. De bij de WIPO aangesloten lidstaten beslissen dan volgens het intergouvernementele principe (er moet een unaniem besluit komen) welke wet- en regelgeving zij willen.

De verwachting is dat dit soort grensoverschrijdende samenwerking uiteindelijk uitmondt in het overdragen van bevoegdheden van de aangesloten lidstaten naar het supranationale niveau. Er is dan in feite sprake van een spill-over van effecten. Nationale staten hevelen in dit voorbeeld slechts een aantal functionele elementen over naar het supranationale niveau (harmonisatie) en houden op

die manier hun soevereiniteit zo goed mogelijk in stand. De stap die daarna nog gezet moet worden is die van regelgeving naar handhaving. Dat moet namelijk ook de grens over en vereist dus wereldwijde samenwerking tussen opsporingsorganisaties.

De aanbeveling aan de Nederlandse overheid is dan ook om er bij de Europese Commissie op aan te dringen om op zoek te gaan naar samenwerking die ook over de grenzen van de Europese Unie heen gaat. En als toevoeging op deze aanbeveling zou er dan direct gewezen kunnen worden op de WIPO als mogelijk instituut waarbinnen deze grensoverschrijdende samenwerking tot stand zou kunnen komen.

De samenwerking die binnen dit instituut gebundeld moet worden bestaat niet alleen uit samenwerking tussen nationale staten, maar moet ook ruimte bieden voor ISP's, bedrijfsleven, consumentenorganisaties en direct marketeers. De aanpak moet bestaan uit een combinatie van mogelijke spambestrijdingsmaatregelen: wet- en regelgeving (en daadwerkelijke handhaving daarvan), zelfregulering (waar mogelijk), technische filters en voorlichting.

Hoofdstuk 1
Inleiding

1.1 Spam!

Drie miljoen dollar in contanten, twintig miljoen dollar op diverse bankrekeningen, luxe auto's zoals een Lamborghini, een Rolls Royce, een Ferrari en een Bentley en een flinke hoeveelheid juwelen. Eén en ander met een totale waarde van ongeveer 30 miljoen dollar. Dit zijn de bezittingen van een drietal Amerikanen (moeder, zoon en een vriend) die in 2002 werden opgepakt door de federale politie in Arizona.[2] Hoe zij aan al die rijkdom en luxe kwamen? Simpel: door het versturen van ettelijke miljoenen e-mails. Het gaat hier natuurlijk over ongevraagde e-mail, kortweg 'spam' genoemd, een woord dat op www.google.com maar liefst 19.500.000 hits oplevert.[3]

Het klinkt te mooi om waar te zijn, maar het versturen van 'spam' of 'unsolicited bulk e-mail' met als doel producten of diensten aan te prijzen en te verkopen is uiterst lucratief. Spammers versturen vaak miljoenen e-mails per zogeheten spamrun (een serie spam e-mails) en zelfs wanneer maar 0,001% van de ontvangers daadwerkelijk het product aanschaft dat in de e-mail wordt aangeprezen, dan kan zo'n spamrun al winstgevend zijn. Als een spammer Viagra pillen wil slijten en hij mailt zijn 'advertentie' naar 10 miljoen e-mailadressen, dan betekent een reactie van 0,001% dat 100 mensen het product willen kopen. Meestal à raison de 50 EUR per pakketje. Dat het percentage kopers veel hoger is dan die 0,001%, blijkt uit de bezittingen van spammers die uiteindelijk opgepakt

[2] Reuters (2002)
[3] Het resultaat van een zoekopdracht op het woord 'spam' op www.google.com op 7 mei 2004

worden, zoals hierboven geschetst. En in een ander voorbeeld: Netmagazine wired.com maakte in 2003 melding van een lijst met gegevens van mensen die hadden gereageerd op een spam e-mail:[4]

> *'An order log left exposed at one of Amazing Internet Products' websites revealed that, over a four-week period, some 6,000 people responded to e-mail ads and placed orders for the company's Pinacle herbal supplement. Most customers ordered two bottles of the pills at a price of $50 per bottle. (…) [In a four week period] Amazing Internet Products would have grossed more than half a million dollars from Goringly.biz, one of several sites operated by the company to hawk its penis pills.'*

Een half miljoen dollar verdienen in vier weken tijd naar aanleiding van 6000 bestellingen is niet mis.

Ongevraagd e-mails krijgen hoeft natuurlijk niet erg te zijn, als de ontvangers van die e-mails daar verder geen problemen mee hebben. Maar dit geldt niet voor het overgrote deel van de ontvangers. Uit onderzoek van Interview NSS uit 2002 blijkt dat maar liefst 85,2% van de Nederlanders -uit een steekproef met 15.000 respondenten- ongevraagde e-mail als irritant beschouwt.[5] Voor het gros van de ontvangers zijn deze e-mails een plaag, een dagelijkse realiteit waar inmiddels honderden miljoenen mensen wereldwijd last van hebben. Het verwijderen van de ongewenste e-mails kost consumenten en werknemers soms veel tijd: het uit elkaar houden van gewone e-mail en spam kan erg lastig zijn door de onderwerpregels van de spamberichten, die vertrouwd en gewoon over kunnen komen. Iedereen wil natuurlijk voorkomen dat gewone e-mails per ongeluk verwijderd worden.

[4] McWilliams (2004)
[5] Interview-NSS (2002)

Toen ik in 1995 mijn eerste stappen op het internet zette bestond spam al zeventien jaar[6], maar daar was toen nog niets van te merken. Vrolijk verspreidde ik mijn e-mailadres op het internet en pas na enige jaren begonnen de eerste spam e-mails binnen te druppelen. Inmiddels zit ik bijna negen jaar op het internet en op mijn diverse e-mailadressen komen dagelijks totaal rond de 1000 spamberichten binnen. Waar bij vermeld moet worden dat dit nog geen jaar geleden minstens zes keer zo weinig was. Het houdt mij dusdanig bezig, letterlijk en figuurlijk (talloze malen drukte ik reeds op de delete knop), dat ik heb besloten om mijn scriptie geheel aan spambestrijding te wijden.

Naast de persoonlijke overlast die ik van spam ondervind, ben ik van mening dat spambestrijding een maatschappelijk en publiek belang is dat snel op een correcte en effectieve manier opgepakt moet worden. De Organisation for Economic Co-Operation and Development (OECD) meldt dan ook op haar website over spam: '*Spam undermines user trust online, reduces firm productivity, and increases costs for Internet service providers. Spam implicates data privacy and consumer protection laws, and spreads computer viruses*'.[7] De OECD heeft dan ook een spam workshop gehouden en heeft tevens diverse rapporten en andere publicaties geschreven over het onderwerp.[8] Ook de World Intellectual Property Organisation (WIPO) noemt met name de wetgeving die noodzakelijk is om spam te bestrijden, die volgens haar 'currently accounts for over half of global e-mail traffic'.[9] Erkenning van spam als een maatschappelijk en publiek probleem blijkt in Nederland het meest direct uit de oprichting van www.spamklacht.nl, een online meldpunt voor spam dat door de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) in het leven is geroepen. Dit is een direct gevolg van de inwerkingtreding van de nieuwe Telecommunicatiewet in 2004. Particulieren kunnen op www.spamklacht.nl klachten indienen tegen overtreders van het spamverbod (artikel 11.7 Tw).

---

[6] Templeton, Brad (2003) Reaction to the DEC Spam of 1978
[7] OECD (2005)
[8] Zie bijvoorbeeld 'Report on non-OECD countries 'Spam Legislation' van Petr Piškula en Jana Klaschková (2004) en het verslag van de OECD Workshop on Spam uit 2004. Beide zijn te vinden op http://www.oecd.org/findDocument/0,2350,en_2649_22555297_1_119666_1_1_1,00.html.
[9] WIPO (2005)

Ondanks alles blijkt in de praktijk het aantal spam e-mails vooralsnog alleen maar te groeien, wat niet zo vreemd is als je de gigantische bedragen bekijkt die het spammen oplevert. En dat ook nog eens gecombineerd met de extreem lage kosten die een spammer in vergelijking met traditionele post moet maken om zijn e-mails te versturen. De bestrijding van spam wil dus nog niet echt lukken. De vraag waarom dat zo is –en wat daar eventueel aan gedaan kan worden- zal centraal staan in mijn scriptie.

1.2 Wat is spam?

De meeste internetters zijn wel bekend met het fenomeen spam. Vrijwel iedereen ontvangt wel eens een e-mail waarin verre reizen, hypotheken, viagra-, valium- en Xanaxpillen, kabel TV, online gokken en andere producten en diensten worden aangeboden. De belangrijkste kenmerken van dit soort berichten zijn:

- het ongevraagde c.q. ongewenste karakter
- de grootschalige verzending (bulk)

Meestal zijn spamberichten ook te herkennen aan hun commerciële inhoud, maar spam kan ook bestaan uit een wervende politieke of charitatieve boodschap (‘Vote X for president!’).

Spam wordt doorgaans gedefinieerd als ‘unsolicited bulk e-mail’ (UBE), oftewel: mail die in grote hoeveelheden (bulk) en ongevraagd (unsolicited) wordt verstuurd. Ongevraagd houdt in dat de ontvanger geen aantoonbare en expliciete toestemming heeft gegeven voor de verzending van de e-mail. De bewijslast ligt bij de verzender en de toestemming is niet overdraagbaar aan derden. Dat wil zeggen dat het niet mogelijk is om een derde persoon of instantie te machtigen om iemand aan te melden voor een mailinglijst. Bulk houdt in

dat de e-mail onderdeel is van een grotere hoeveelheid e-mails, die elk voor een wezenlijk deel identiek zijn.[10] Er wordt gesproken van 'unsolicited commercial e-mail' (UCE) als de nadruk ligt op het commerciële karakter van de e-mail.

Een e-mail hoeft niet ongevraagd en bulk te zijn om het als spam te kunnen kwalificeren. De combinatie ongevraagd/bulk is de meest voorkomende variant en meestal een voldoende voorwaarde om als spam gekwalificeerd te worden, maar geen noodzakelijke. Bulkverzendingen zijn een normaal geaccepteerd verschijnsel. Het gaat dan bijvoorbeeld om mailinglijsten en nieuwsbrieven. Ook ongevraagde e-mail is gebruikelijk. Hierbij valt te denken aan het stellen van vragen aan een webmaster die iemand kan hebben naar aanleiding van een site-bezoek. Andersom is het echter ook zo dat een e-mail die in bulk verzonden wordt als spam gekenmerkt kan worden, terwijl hij niet ongevraagd is. De inhoud van de e-mail kan als onwenselijk worden beschouwd. Tevens kan een e-mail die slechts in eenvoud is verstuurd aangemerkt worden als spam, wanneer het een ongevraagde boodschap is die bijvoorbeeld vanwege inhoud of afzender niet wordt gewaardeerd. Het gaat echter bij de meest gangbare definitie van spam niet om de inhoud (content), maar om de goedkeuring van de ontvanger (consent), en dus om de combinatie van de kenmerken ongevraagd en bulk.

Mag het versturen van bulk e-mails zoals politieke oproepen of culturele evenementen of desnoods voor producten als viagra pillen en hypotheekoffertes dan helemaal niet? Jawel, zolang de ontvanger maar vooraf toestemming heeft gegeven om de e-mail te ontvangen. Dit is het zogeheten opt-in principe: vooraf goedkeuring verlenen voor het laten toesturen van bulk e-mails. De e-mail is dan niet meer ongevraagd en valt daardoor niet onder de noemer spam. Dubbel opt-in wil zeggen dat iemand de inschrijving op een maillijst ook daadwerkelijk bevestigt. Opt-in is het tegenovergestelde van opt-out, waarbij in elke e-mail de optie wordt geboden om uitgeschreven te worden. Maar de e-mail is dan dus al binnen.

[10] Spamvrij (2004)

De definitie van spam roept nogal wat vragen op. Naast de miljoenen mensen die viagra e-mails alleen maar razend irritant vinden, zijn er ook mensen die wel prijs stellen op de e-mails: en dat is derhalve de doelgroep van de spammers. Het is tevens de vraag welke definitie van spam precies gehanteerd wordt door spammers, consumenten, ISP's (Internet Service Providers) en overheden. Regelgeving blijkt onder andere erg lastig te zijn doordat veel landen spam op een andere manier definiëren. In hoofdstuk twee zal ik verder ingaan op de problemen met de definitie van spam.

Oorsprong

De herkomst van het woord spam is te herleiden tot twee mogelijke verklaringen. In een sketch uit de jaren zeventig van het Britse televisie- programma Monty Python proberen een man en een vrouw iets te eten te bestellen. In letterlijk elk gerecht blijkt spam te zitten (eggs and spam, eggs, bacon and spam, eggs, spam, spam and beans and spam, etc.). Aan de ober vragen *waarom* in elk gerecht spam zit blijkt onmogelijk: elke keer als de twee het woord 'spam' noemen begint een groep Vikingen die verderop in het restaurant zit luidkeels 'spam, spam, spam' te zingen.

De andere verklaring betreft het ingeblikte vlees van de firma Hormel dat de naam spam draagt. Volgens de 'legende' zou de voedingswaarde van spam vrijwel nihil zijn: veel massa, weinig inhoud. De Australische website smh.com meldt echter dat spam niet voor niets als sinds 1937 bestaat.[11] Sinds het door Hormel werd ontwikkeld in 1937, heeft spam zich over de hele wereld verspreid. In de Tweede Wereldoorlog was het een bron van eiwitten voor de geallieerde soldaten. Premier Nikita Chroestjov schijnt gezegd te

[11] AFP (2004)

hebben: "zonder spam zouden we het leger niet hebben kunnen voeden." Hormel zelf wijst naar de Monty Python sketch als de bron van het kwaad.[12]

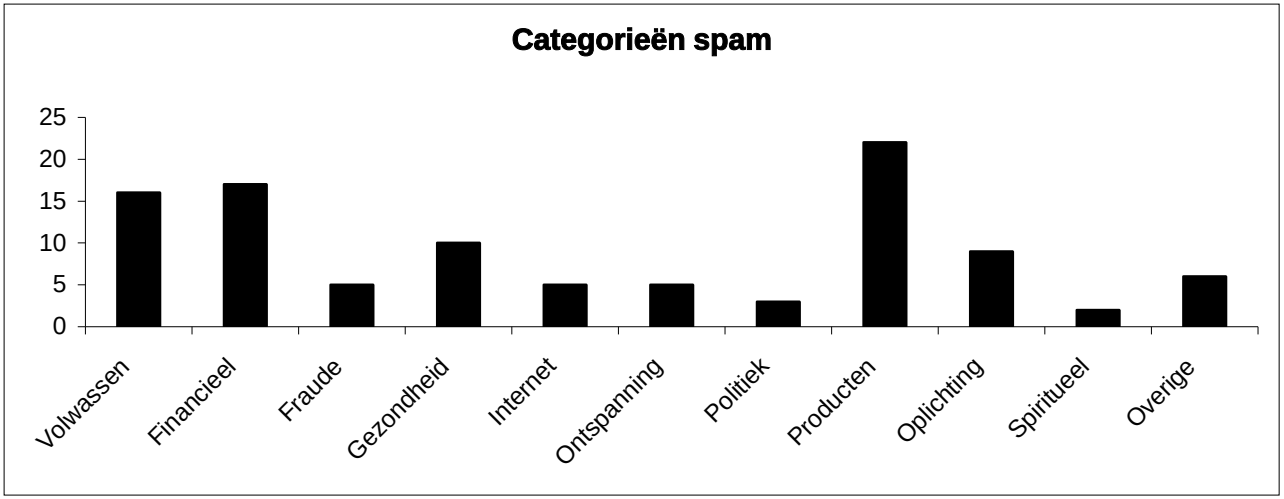
Een van de eerste spam e-mails werd al in 1978 verstuurd. Internetgoeroe Brad Templeton beschreef de aanleiding van die eerste spam e-mail op zijn website:[13]

> *'The sender is identified as Gary Thuerk, an aggressive DEC marketer who thought Arpanet users would find it cool that DEC had integrated Arpanet protocol support directly into the new DEC-20 and TOPS-20 OS. I spoke with him to get his reflections on the event. (…) Thuerk thought, and maintains to this day that he didn't think he was doing anything wrong -- even though he gets a moderate amount of spam on his current E-mail account. He felt the Dec-20 was really relevant news to the Arpanet community, the first major system with Arpanet software built into it. Indeed, some of those who commented on the message felt it was definitely more of interest than other small mass mailings they had seen, with baby announcements and personal trivia.'*

De term spam werd pas echt bekend in 1994, toen twee advocaten zichzelf wilden aanprijzen met betrekking tot een komende 'green card lottery'. Zij lieten iemand een script schrijven dat de boodschap vervolgens naar alle nieuwsgroepen op Usenet (een online communicatiesysteem) verstuurde. Dat waren er rond die tijd ongeveer 12.000. In de veelal boze reacties op het bericht viel het woord spam al snel en verspreidde zich in korte tijd over de hele wereld.[14]

---

[12] Op http://www.spam.com/ci/ci_in.htm beschrijft Hormel de ontstaansgeschiedenis van het woord spam. Daarbij merkt Hormel ook op dat ze het vervelend vinden dat het woord spam een negatieve betekenis heeft. Zolang mensen in kleine letters spam schrijven, is het niet erg, maar SPAM is de merknaam van Hormel. Daar moet iedereen van afblijven. Gezien op 15 juni 2004.
[13] Templeton, Brad (2004) The first spam e-mail
[14] Templeton, Bad (2003) The origins of spam



Er zijn verschillende categorieën spam. Brightmail, een Amerikaans bedrijf dat zich volledig op spambestrijding en monitoring heeft gestort, analyseert op maandelijkse basis hoe de verdeling er globaal uitziet. Voor mei 2004 was dat als volgt[15]:

Deze verdeling is al vrij lang ongeveer hetzelfde. De categorie 'Producten' is het grootste, maar beslaat dan ook het meest uitgebreide scala aan mogelijkheden. Van make-up tot zogeheten 'investigation services' en van kleding tot huishoudelijke apparaten. Een goede tweede en één van de oudste categorieën is het kopje 'Volwassen', waar onder andere porno-advertenties onder vallen. Opvallend is

[15] Brightmail (2004) Spam statistics May 2004

dat ‘Gezondheid’ slechts 10% van het totale spamarsenaal beslaat. Het aantal aanbiedingen voor penisverlengers en Viagrapillen lijkt als je de klachten hierover hoort vaak veel groter te zijn dan hier wordt gesuggereerd.

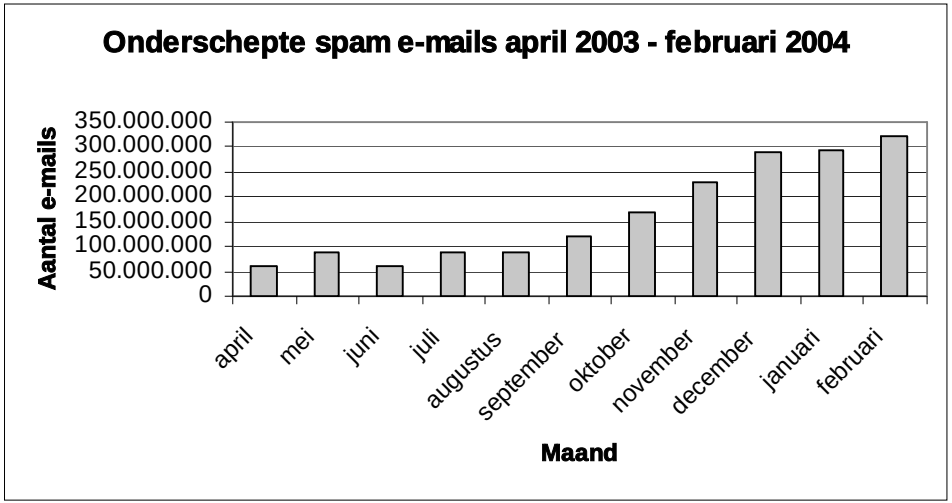
1.3 Wat is het probleem met spam?

Zoals uit de inleiding blijkt beschouw ik spam zelf als een probleem: een discrepantie tussen de werkelijkheid (meer dan 1000 spam e-mails per dag) en een door mij gewenste situatie (0 spam e-mails per dag). Maar spam wordt niet door iedereen als een probleem beschouwd. Spammers verdienen veel geld met hun bezigheden en zij zullen spam dus niet als een probleem beschouwen, maar juist als een oplossing voor bijvoorbeeld hun geldproblemen. En tevens als een simpele manier om snel geld te verdienen. Daarbij moet overigens ook nog eens een onderscheid gemaakt worden tussen soorten spammers. Niet alle spammers proberen simpelweg zoveel mogelijk geld te verdienen door *rücksichtslos* naar alle adressen te e-mailen die ze te pakken kunnen krijgen. Er is ook een categorie die wel aan enigerlei norm wil voldoen (bijvoorbeeld door middel van zelfregulering) om op een legale manier potentiële klanten of geïnteresseerde mensen te benaderen. In hoofdstuk vier kom ik op dit onderscheid terug.

Maar er zijn ook veel gevolgen van spam die wel als probleem worden beschouwd. Spam brengt hoge sociale en economische kosten met zich mee. De sociale kosten zijn hoog voor mensen die veel spam ontvangen en bijvoorbeeld per ongeluk gewone e-mails tegelijk met een lading spam weggooien. Spam verwijderen kost ook veel tijd. Dit kan privé-tijd zijn, maar ook werktijd. Dan gaat het over de economische kosten van spam. De cijfers die genoemd worden met betrekking tot de kosten van spam lopen sterk uiteen in alle artikelen en rapporten die hierover verschenen zijn, maar dat het wereldwijd inmiddels in de miljarden loopt is wel aannemelijk te

maken. Zo moeten bijvoorbeeld internet-providers extra e-mailservers aanschaffen om de gigantische hoeveelheden e-mail te verwerken[16].

Uit diverse onderzoeken blijkt dat van alle e-mailverkeer 37 tot 55% uit spam bestaat.[17] En dit aantal neemt alleen maar toe. Ter illustratie op de volgende bladzijde de aantallen spam e-mails die door MessageLabs (een Amerikaans bedrijf dat zich heeft gespecialiseerd in virusbestrijding) tussen april 2003 en februari 2004 zijn onderschept.[18]



[16] Zo is internetprovider XS4ALL jaarlijks 368.000 EUR kwijt aan extra servers en personeel; Reijnders, Maarten (2002)
[17] Volkskrant (2004) Internet loopt vol met spam, en Smallzine (2004)

Brightmail komt met nog grotere cijfers. Brightmail doet de spamfiltering voor een groot aantal Amerikaanse providers (in mei 2004 scande Brightmail meer dan 100 miljard e-mailberichten)[19] en constateerde in mei 2004 dat 64% van alle door hen gescande e-mails spam was. In juni 2003 was dat nog 49%.[20]

In juli 2003 presenteerde Nucleus Research de resultaten van een onderzoek naar de kosten van spam. Volgens het onderzoek zijn Amerikaanse bedrijven 874 dollar per werknemer per jaar kwijt als gevolg van spam door verloren arbeidsproductiviteit. [21]

De gemiddelde werknemer ontvangt 13,3 spamberichten per dag waaraan hij in totaal 6,5 minuut besteedt. De onderzoekers gaan bij de berekening van het uiteindelijke schadebedrag uit van een uurloon van 30 dollar en 2080 werkuur per jaar. Dit komt neer op een verlies van 1,4% arbeidsproductiviteit per jaar als gevolg van spam.[22]

Het artikel op webwereld.nl waarin melding werd gemaakt van bovenstaand onderzoek gaat verder en meldt:

> *'Het onderzoek van Nucleus staat niet op zichzelf. Onlangs kwam Network Associates tot de conclusie dat de gemiddelde internetter veertig minuten per week kwijt is aan spam. Begin dit jaar becijferde Ferris Research al dat bedrijven en providers wereldwijd op jaarbasis bijna twaalf miljard dollar kwijt zijn aan het verwerken en tegengaan van spamberichten.'*

---

[18] Messagelabs (2004)
[19] Brightmail filtert voor o.a. AT&T WorldNet, EarthLink, MSN, Verizon Online, en een aantal 'Global 2000 corporations'.
[20] Brightmail (2004) Spam statistics June 2004
[21] Nucleus Research (2003)
[22] Verhagen, Laurens (2004) Schadepost spam: 874 dollar per werknemer

Door de grote hoeveelheden spam raken mailboxen steeds vaker verstopt. Veel mensen hebben een gratis account bij bijvoorbeeld Hotmail of Yahoo. Over het algemeen kunnen die mailboxen maximaal één a twee MB (Megabyte) aan informatie opslaan. Bij grote hoeveelheden spam en/of virussen raken mailboxen sneller vol. Zodra een mailbox vol zit, komt nieuwe mail niet meer binnen. Die gaat dan onverrichterzake retour afzender. Dit levert twee problemen op. Ten eerste komt de e-mail niet aan bij de geadresseerde, waardoor economische of sociale schade op kan treden. Ten tweede zal de eigenaar van de mailbox maatregelen moeten nemen, zoals het instellen van spamfilters, of wanneer dat niet afdoende helpt: tegen betaling de mailboxruimte laten vergroten. Dit levert derhalve weer extra economische kosten op.

De economische kosten van spam zijn dus zeer hoog. Daarnaast belemmert spam de informatie uitwisseling op het internet. Communicatie wordt verstoord of vertroebeld en de e-mail infrastructuur van het internet lijkt soms onder de druk te gaan bezwijken. Bij een voortdurende toename van het aantal spam e-mails zullen de kosten van het transporteren van een e-mail exponentieel mee stijgen. Deze kosten worden momenteel afgewenteld op de ontvanger, daar de verzenders van spam e-mails nauwelijks gepakt (kunnen) worden.

En ook privacy is een issue. Hoe komen spammers aan e-mailadressen om te spammen? En is de ongewenste bezorging van spam e-mails geen inbreuk op de privacy van de ontvanger? Ook wordt ‘Phishing’ een steeds groter probleem. Hierbij ontfutselen spammers door het in de look-and-feel namaken van e-mails van legitieme bedrijven persoonsgegevens van gebruikers, waarna ze die gegevens misbruiken, voor bijvoorbeeld het stelen van creditcard gegevens.

In hoofdstuk twee wordt dieper ingegaan op de vraag welke elementen te benoemen zijn waardoor spam als probleem te definiëren valt en wat de problemen zijn met het vaststellen van een eenduidige definitie.

1.4 Probleemstelling

De doelstelling van mijn scriptie is om te analyseren wat anno 2004 de problemen zijn met betrekking tot spambestrijding en hoe overheden met spambestrijding omgaan. Uit deze analyse wil ik conclusies trekken en aanbevelingen doen om spambestrijding waar mogelijk effectiever te laten verlopen. Het gebrek aan consensus over de definitie van spam, over het precieze probleem en zelfs over de mogelijke oplossingen zal nog wel even voortduren. In de tussentijd raakt menig e-mailbox steeds verder verstopt. De precieze definitie van spam en de duiding van de probleemgebieden staan weliswaar ter discussie, maar dat urgentie vereist is in de aanpak van spam, daar is iedereen het wel over eens.

Vraagstelling

De vraag die centraal staat in mijn poging om de door mij gestelde doelstelling te bereiken is:

Kan de overheid een rol spelen met betrekking tot spambestrijding, en zo ja: voor welke overheid is welke rol weggelegd?

Ik zeg hier opzettelijk niet bijvoorbeeld ‘welke Nederlandse overheid’, want het is de vraag of spam wel een probleem is dat op nationaal niveau kan worden opgelost. Internationale ontwikkelingen lijken alles bepalend te zijn voor het doen en laten van de Nederlandse overheid met betrekking tot spambestrijding. Verder gaat mijn scriptie alleen over digitale spam: ongevraagd drukwerk per *snailmail* (conventionele postbestelling) komt niet aan de orde.

1.5 Opzet onderzoek

In deze scriptie zijn drie onderzoeksmethoden gebruikt. Dit zijn literatuuronderzoek, expertinterviews en praktijkonderzoek. Het uitgangspunt voor mijn scriptie was mijn ervaring uit de praktijk. Ik werk al jaren bij internetprovider XS4ALL en heb daardoor veel directe ervaring met spamproblemen. Niet alleen op technisch vlak, maar ook op juridisch vlak door de rechtzaken die XS4ALL voerde tegen spammer AbFab (en won) en op maatschappelijk vlak, door mijn betrokkenheid bij Bits of Freedom, een digitale burgerrechten organisatie die is opgericht door twee ex-XS4ALL medewerkers. Tijdens mijn stage bij European Public Policy Advisers (EPPA) volgde ik ontwikkelingen op spamgebied eveneens van nabij (wet- en regelgeving, nieuwsberichten in de media e.d.), omdat zij de Dutch Direct Marketing Association (DDMA) als klant hebben. Dat was een interessante zijsprong, daar ik niet eerder met spammers zelf in aanraking was geweest (zij beschouwen zichzelf niet als spammer, maar de wet heeft inmiddels anders beslist in gevallen waarin bij de DDMA aangesloten bedrijven ongevraagde e-mails verstuurden).

Voortbouwend op de empirische basis zocht ik in literatuuronderzoek bevestiging of weerlegging van mijn theorieën over spam(bestrijding). Ik heb daarbij gebruik gemaakt van nieuwsberichten uit zowel conventionele als digitale media, onderzoeken en rapportages van (inter- en supra)nationale instituties, wetenschappelijke literatuur en wet- en regelgeving.

Ten slotte heb ik een aantal ongestructureerde kwalitatieve interviews gehouden met diverse actoren, met name om de technische achtergrond van spambestrijdingsmogelijkheden goed te doorgronden. Scott McIntyre, Daniel Resoort, Cor Bosman en Mick Switser van de technische afdeling bij Xs4ALL zijn hierin onmisbaar geweest. Ook heb ik gesproken met Sjoera Nas van Bits of Freedom en Judith van Erve van het Instituut voor Informatierecht van de Universiteit van Amsterdam, om respectievelijk de politieke en juridische implicaties van spam beter te begrijpen en de ontwikkelingen op die gebieden beter te kunnen plaatsen. Mijn bevindingen uit die gesprekken heb ik gebruikt om de structuur van mijn scriptie mee vast te stellen en om richting te geven aan mijn argumentatie.

Letterlijke of algemene weergaves van de gesprekken zijn niet opgenomen in deze scriptie, daar zij slechts de achtergrond vormden voor het vormen van mijn mening en argumentatie. Alleen van mijn gesprek met Scott McIntyre zijn vrij letterlijke weergaves opgenomen in het technische deel van de werking van spam in hoofdstuk 2.

1.6 Relevantie

Zoals gezegd in paragraaf 1.3: spam irriteert, het kost veel tijd en geld om het te verwijderen, het verstoort de communicatie op internet doordat reguliere e-mails zoek kunnen raken tussen de vele spam e-mails en het kan beschouwd worden als een aanval op de privacy van internetgebruikers. Het idee om de problemen in kaart te brengen met betrekking tot spambestrijding en het aandragen van mogelijke oplossingen om de aanpak hiervan beter te laten verlopen, is alleen al om die redenen van belang. Als ik –hoe gering mijn bijdrage ook is- de bij het spamprobleem betrokken actoren (handelende personen of instanties) kan adviseren over een effectievere aanpak van spambestrijding, dan doe ik dat graag.

Daarnaast is spam door het grensoverschrijdende karakter ook een interessante casus voor het toetsen van wetenschappelijke theorieën aan de praktijk. Ik doel hiermee op de netwerkbenadering, die ik zal gebruiken als theoretisch kader in mijn scriptie (zie hs 3). De keuze hiervoor is eenvoudig te verklaren: spam heeft niet alleen gevolgen die geproblematiseerd worden, maar is zelf ook weer een gevolg van een ander probleem. Het internet is feitelijk hét ideaal-typische netwerk. Spam overschrijdt bestaande territoriale grenzen en dat heeft gevolgen voor het handelingsvermogen van nationale staten. Zij zijn immers instrumenteel gebonden aan territoriale grenzen. Samenwerking tussen nationale staten lijkt derhalve onvermijdelijk om tot een oplossing van het spamprobleem te komen. Het is interessant om te kijken of de handvatten die de netwerkbenadering hiervoor biedt bruikbaar zijn.

En voortbordurend op de bruikbaarheid van de netwerkbenadering bij spambestrijding: spam is niet het enige ICT-gerelateerde probleem dat een grensoverschrijdend karakter heeft waardoor actoren zich als onderdeel van wereldwijde netwerken terugvinden. De manier van aanpak van het spamprobleem is wellicht ook toepasbaar op soortgelijke problemen, zoals de aanpak van het illegaal kopiëren van software.

1.7 Indeling hoofdstukken

De opbouw van deze scriptie is als volgt. In **hoofdstuk twee** vertel ik meer over de werking van e-mail in het algemeen en spam in het bijzonder. Tevens ga ik in op de vraag hoe spam in de loop der jaren is geëvolueerd. Hierbij wordt duidelijk dat spammers de digitale verdedigingsmechanismen van spambestrijders steeds weten te ontlopen of voor te blijven door allerlei technische trucs. Ook wordt in dit hoofdstuk alvast aangestipt dat de bestrijding niet alleen om technische redenen faalt, maar ook omdat er geen sprake is van sluitende wet- en regelgeving en de daarbij behorende handhaving van die wet- en regelgeving. En dat heeft onder andere weer te maken met het gebrek aan een eenduidige definitie van spam. Om die reden probeer ik te ontleden hoe spam nu precies valt te definiëren.

In **hoofdstuk drie** geef ik een reflectie op de reeds bestaande methoden van spambestrijding en hun effecten. Achtereenvolgens komen de technische, economische, juridische en communicatieve aanpak aan bod. Daarna volgt nog een stukje over de (on)mogelijkheden van zelfregulering, waarna ik afsluit met de effectiviteit van alle methoden en hun eventuele beperkingen.

In **hoofdstuk vier** wordt voor het eerst hardop de vraag gesteld hoe het komt dat de huidige methoden van spambestrijding niet volstaan. Wat is de theoretische achtergrond die hier een verklaring voor kan bieden? Ik constateer dat er in de huidige samenleving

waarin grenzen verdwenen zijn steeds meer horizontale relaties tussen actoren ontstaan waardoor gezagsverhoudingen worden aangetast. Er is sprake van deterritorialisering, interacties tussen mensen blijken niet meer eenduidig toe te schrijven aan een specifiek en daarbij passend rechtsregime. Actoren bevinden zich in netwerken waarin zij wederzijds afhankelijk van elkaar zijn in het komen tot oplossingen voor tal van complexe vraagstukken. Onzekerheid over andere actoren, hun percepties en hun belangen, neemt een centrale plaats in bij besluitvormingsprocessen. Hoe die onzekerheid te reduceren valt om tot samenwerking tussen actoren te komen, wordt dan ook in dit hoofdstuk uitgelegd. Tevens probeer ik theoretische handvatten te geven om een antwoord te kunnen geven op de vraag: 'hoe manage je een netwerk?'

In **hoofdstuk vijf** komen vervolgens alle bij spam betrokken actoren en hun belangen en percepties aan bod. Hiermee probeer ik vragen te beantwoorden als: Waar gaat spambestrijding op organisatorisch gebied precies mis? Waarom komt samenwerking niet van de grond? Waarom neemt niemand het voortouw in het spambestrijdingsproces? Hier probeer ik dus de theoretische bevindingen uit hoofdstuk drie te vertalen naar de praktijk. Is de onzekerheid waar ik het daar over had inderdaad te reduceren en biedt dit voldoende perspectief voor een oplossing van het spamprobleem? Kortom: wordt er bij spambestrijding voldaan aan de voorwaarden die de netwerkbenadering stelt aan een succesvolle manier van het benaderen van een beleidsproces of is de praktijk weerbarstiger?

De combinatie van het in kaart brengen van onzekerheden in het netwerk, het mogelijke perspectief dat reductie van die onzekerheden biedt en de huidige methoden van aanpak, leidt in **hoofdstuk zes** tot een poging om bouwstenen aan te dragen voor een oplossing van de spamproblematiek. Hoe moet het dan wel? Welke obstakels er verwijderd moeten worden om tot een oplossing te komen en hoe dat dan zou moeten komt in dit hoofdstuk aan de orde. Wat in de gewijzigde verhoudingen van de netwerkmaatschappij de rol van de overheid is of kan zijn, wordt eveneens nader belicht.

In **hoofdstuk zeven** ten slotte trek ik de conclusies uit mijn stuk en probeer ik aan de hand van de bouwstenen uit hoofdstuk zes aanbevelingen te doen om het spambestrijdingsbeleid beter aan te pakken. Hier probeer ik antwoord te geven op de centrale vraag uit mijn scriptie, namelijk of de overheid een rol kan spelen met betrekking tot spambestrijding, en zo ja: voor welke overheid is welke rol weggelegd?

Hoofdstuk 2
Spam

2.1 Hoe werkt e-mail?

E-mail (electronic mail) bestaat al meer dan dertig jaar. In 1971 ontwierp Ray Tomlinson de eerste e-mail applicatie voor ARPANET (Advanced Research Projects Agency) dat door het Amerikaanse Department of Defense (DOD) was ontworpen.[23] Met de uitbreiding van het internet werden ook het gebruik van en de technologie achter e-mail steeds verder ontwikkeld.

Er zijn vier kernelementen die essentieel zijn voor de werking van e-mail. Het gaat om de:

- Mail User Agent (MUA)
- Mail Transfer Agent (MTA)
- Mail Delivery Agent (MDA)
- Mail Storage Agent (MSA)

De verzender van een e-mail heeft een programma nodig waarmee hij de e-mail op kan stellen. Dit is de Mail User Agent. Er zijn talloze MUA's op de markt. De meest bekende voorbeelden zijn gebruiksvriendelijke programma's als Outlook, Netscape Mail en Eudora. Maar ook de op het oog meer gecompliceerde mailprogramma's als pine, mutt en elm zijn bruikbaar als MUA.

[23] Crocker, Dave (2004)

Na het opstellen wordt de e-mail verstuurd naar de ontvanger via een transport medium: de Mail Transfer Agent. Dit betreft dan een intranet of het internet. In een intranet wordt de e-mail verstuurd naar computers die in een afgesloten netwerk zitten. Dit betreft dan bijvoorbeeld e-mail in een bedrijfsnetwerk. Als e-mail naar ontvangers buiten een afgesloten netwerk verstuurd wordt, dan kan dit via het gehele internet gaan.

De e-mail wordt vervolgens afgeleverd door middel van een Mail Delivery Agent en opgeslagen op de server van de internet provider van de ontvangende partij, of het wordt direct afgeleverd op de eigen computer van de ontvangende partij. Dit betreft de Mail Storage Agent. De e-mail blijft daar bewaard tot de ontvanger zijn eigen Mail User Agent in werking stelt om de e-mail te lezen en/of te beantwoorden.

Hoe weet een onderdeel van het e-mailsysteem nu waar de e-mail moet worden afgeleverd? Net als bij een gewone brief is de adressering op de envelop van belang. De geadresseerde wordt bij e-mail aangeduid als de ‘TO-header’. Dit moet een bestaand adres zijn. De afzender(de ‘FROM-header’) is net als bij gewone post te vervalsen. Iedereen kan op de virtuele envelop billgates@microsoft.com als afzender invullen en dat is dan ook precies iets waar veel spammers misbruik van maken. Zij doen zich bijvoorbeeld voor als de supportdesk van Microsoft en vertellen nietsvermoedende ontvangers van hun e-mails dat ze een attachment moeten openen, omdat dat zou voorkomen dat ze besmet worden met een nieuw virus (terwijl in die attachment dan juist een virus zit!), of ze worden bijvoorbeeld uitgenodigd om op een link in de e-mail te klikken waardoor de spammer in kwestie weet dat het adres daadwerkelijk in gebruik is, waarna het adres weer op nieuwe spam cd’s wordt gezet en wordt doorverkocht. De technische infrastructuur van het internet is feitelijk te zwak om dit soort misbruik te vo0rkomen. Het enige waar internet protocollen naar kijken is of de domeinnaam (het deel van een e-mailadres na het @-teken, bijvoorbeeld microsoft.com) van de afzender bestaat op het internet. Er kan niet gecheckt worden of die domeinnaam daadwerkelijk van de afzender is. Dit werkt namelijk hetzelfde als bij gewone post: op een brief kun je makkelijk een ander adres als afzender zetten dan in werkelijkheid het geval is. Het enige verschil is dat bij het

versturen van gewone post per brief betaald moet worden, terwijl het versturen van e-mail nagenoeg gratis is, het is dus veel makkelijker en goedkoper om e-mail als spam medium in te zetten dan conventionele post.

Het adres van de ontvanger moet in ieder geval wel bestaan, anders komt de e-mail onbestelbaar retour. Identificatie van een gebruiker hangt af van drie onderdelen van een e-mail adres: het user ID (User Identification Code), het scheidingsteken @ en een domeinnaam, die de computer identificeert op het internet. De user ID is in feite de persoonlijke adressering. Meestal is dit de naam van de ontvanger. Om billgates@microsoft.com weer als voorbeeld te nemen: hierbij is billgates de user ID. De @ geeft aan dat de user ID eindigt en dat vervolgens de locatie van de user bepaald moet worden. Dit betreft de domeinnaam, die in dit geval microsoft.com is.

Niet alle domeinen accepteren alle e-mail. Indien dit wel het geval is, is er sprake van een *catch-all* domein. Dit houdt in dat alle e-mail voor een domeinnaam (@domeinnaam.nl) die niet voor de overige e-mailboxen op die domeinnaam bedoeld is, hierin uitkomt. Er kan ook voor worden gekozen om alleen e-mail te accepteren van adressen die daadwerkelijk op een domeinnaam ingesteld zijn. Als een gebruiker jan@microsoft.com en piet@microsoft.com heeft aangemaakt, maar niet koos@microsoft.com, dan zal e-mail naar dat laatste adres bouncen. Bouncen betekent dat de e-mail onverrichterzake retour afzender gaat. *Address Unknown.*

De adressering is terug te vinden in de ‘header’ van een e-mail. Daarin staan de gegevens van de afzender, de ontvanger en de op het internet afgelegde route naar de ontvanger. Daarnaast is er de ‘body’ van een e-mail. Hierin wordt de informatie opgeslagen die verstuurd moet worden. Dit kan platte tekst zijn, of een attachment. Elk onderdeel van een e-mail krijgt de header informatie opgeplakt. In theorie kan een e-mail wanneer deze over grote afstand verstuurd wordt tijdens de virtuele rit opgesplitst worden in meerdere delen. Eén deel reist bijvoorbeeld via een machine in China, terwijl een andere deel de route via Noord-Amerika neemt. Pas als alle

onderdelen van de e-mail weer bij elkaar zijn en de headerinformatie geheel compleet is, wordt de e-mail afgeleverd. Dit duurt doorgaans hooguit enkele seconden.

Niet alleen de mogelijkheid tot het vervalsen van de 'FROM-headers' is van belang voor de spamproblematiek, het gaat vooral ook om de optie om mail BCC te versturen. BCC staat voor 'blind carbon copy'. Bij het versturen van een e-mail zijn er drie opties wat betreft de adressering:

1. TO: als er direct naar één persoon gemaild wordt, dan wordt het e-mail adres van die persoon doorgaans in de TO: regel gezet.
2. CC: Bij e-mailen naar meerdere personen is de optie CC (carbon copy) gebruikelijk. Er wordt dan een kopie van de e-mail doorgestuurd naar de overige adressen. De ontvangers zien ook alle andere adressen die in de CC-header staan.
3. BCC: Indien de verzender de privacy van de ontvangers wil beschermen kan hij gebruik maken van de BCC-optie, waarbij het voor geen enkele ontvanger zichtbaar is naar wie de e-mail allemaal gestuurd is. De ontvanger kan alleen maar zien wie er in de TO en CC-header staan vermeld.

Veel spammers e-mailen naar duizenden of miljoenen mensen tegelijk door ze in de BCC-header te zetten. Dit is bij veel mensen niet bekend, waardoor internet providers veel vragen krijgen van mensen die zomaar e-mails ontvangen die op het eerste gezicht helemaal niet aan hen geadresseerd zijn. Zij zien immers alleen de adressen in de TO en/of CC-header. Hun eigen adres staat daar niet in, die staat immers in het voor hen onzichtbare BCC-veld.

2.2 Hoe werkt spam?

Spam versturen is niet ingewikkeld. In principe kan iedereen met een internetaansluiting spam versturen. Aan adressen komen om te spammen is eenvoudig. Spammers 'harvesten' (oogsten) op internet e-mailadressen met behulp van spamrobots: dit zijn programma's die continu op zoek zijn naar alles op het World Wide Web waar een @-teken in voorkomt. Daarnaast zijn er diverse cd's in omloop met duizenden of zelfs miljoenen e-mailadressen, die tegen zeer geringe bedragen te koop zijn.

Ook zijn er software programma's die lukraak cijfer- en lettercombinaties uitproberen: aaa@microsoft.com, aab@microsoft.com, aac@microsoft.com, etc. In korte tijd worden er op deze manier miljoenen adressen gefabriceerd, waarvan het gros niet zal bestaan, maar veel adressen ook wel. Met name bij domeinnamen als hotmail.com waarvan bekend is dat er potentieel vele miljoenen adressen onder hangen is het interessant voor spammers om deze methode te gebruiken.

Vervolgens hebben spammers een programma nodig om hun spamrun mee te versturen. Deze kunnen door henzelf gemaakt worden, of worden aangekocht. Er worden –door spammers!- zelfs software programma's verkocht die op een eenvoudige wijze grote aantallen e-mails kunnen versturen. Op 3 maart 2004 ontving ik zo'n spam e-mail:

> *Dark Mailer is a super fast bulk email software that sends out at speeds greater than 1,000,000 emails per hour* on a dedicated mailing server. Dark Mailer has the capability to use Proxies and Relays and also to send directly.*[24]

[24] Zie bijlage A

Een bronvermelding van deze e-mail is niet eens mogelijk: de afzender heeft weten te maskeren waar hij/zij zich werkelijk bevindt, iets wat spammers vrijwel altijd doen.

Het probleem met spam ontstaat na de aflevering: de e-mail is op het juiste adres afgeleverd, maar de ontvanger van de e-mail wil niets te maken hebben met de gestuurde mail. De mail wordt door de ontvanger als ongewenst beschouwd. Klagen heeft echter geen zin, want als de ontvanger terugmailt naar het adres waar de spam e-mail vandaan kwam, dan levert dat in de praktijk vaak een niet bestaand adres op: de afzender blabla@microsoft.com blijkt bijvoorbeeld vervalst te zijn. Maar het kan nog erger: in veel spamberichten staat netjes een link met als kopje ‘unsubscribe’. Als de nietsvermoedende lezer hier echter op klikt, dan weet de spammer dat het e-mailadres daadwerkelijk ook wordt gelezen, waarna het adres wordt doorverkocht aan weer andere spammers. Het is dus eenvoudig om op een spamlijst te komen. Maar er weer af komen is zo goed als onmogelijk.

En een Nee/Nee sticker op de digitale brievenbus plakken is een stuk ingewikkelder dan bij gewone post. Bij dat laatste zal de persoon die de post aflevert zich aan de opdracht NEE houden, omdat hij anders boze klachten krijgt: de verzender van de post (vaak reclamemateriaal) is meestal eenvoudig te achterhalen. Alleen als de post een zichtbare adressering bevat mag de postbode het bericht afleveren. Maar bij e-mail is het zoals gezegd lastiger. De aflevering van e-mail wordt geregeld door de ISP van de ontvangende klant. De ISP kijkt net als de postbode niet naar de inhoud het bericht, maar slechts naar het ontvangstadres en of de afzender zou kunnen bestaan, zoals eerder geschetst. En de BCC-header is weliswaar niet zichtbaar voor de ontvanger, maar bestaat wel degelijk. De ISP levert dus per definitie alleen maar post af waar een adres op staat. Ongeadresseerde spam bestaat niet in de virtuele wereld.

Een Nee/Nee sticker kan in de digitale wereld daarom hooguit uit een spamfilter bestaan. Een spamfilter kijkt naar de afzender (kan die bestaan en levert die verzender doorgaans betrouwbare e-mail af) en soms ook naar de inhoud. Als de spam e-mail slim is opgesteld glipt hij door deze filters heen en wordt hij gewoon afgeleverd.

Spammers zijn niet geïnteresseerd in boze reacties. Ze zijn alleen geïnteresseerd in kopers van hun product of dienst. In één spamrun sturen ze hun berichten soms naar wel tien miljoen geadresseerden. Daarvan komen honderdduizenden of zelfs miljoenen e-mails onverrichterzake retour omdat de betreffende e-mailadressen bijvoorbeeld niet meer bestaan. Naar schatting zullen duizenden mensen boos reageren en al die reacties zijn alleen maar lastig voor spammers. Het nepadres dat ze gebruikt hebben om hun e-mail vanaf te versturen zullen ze –als het al bestaat- dus nooit bekijken. Wat ze wel doen, is in de e-mail wijzen op een website waar je de producten kunt bestellen. Bestellingen die op die website geplaatst worden, worden opgeslagen in een database of ze worden naar de spammers gemaild. Dit betreft dan natuurlijk een ander e-mailadres dan het adres dat voor de spamrun werd gebruikt.

Evolutie van spam

Natuurlijk wordt er geprobeerd om de honderden miljoenen spam e-mails tegen te houden. De meest recente ontwikkeling op technisch gebied is bijvoorbeeld SpamAssassin. Hier zal ik later uitgebreider op terugkomen, maar het geeft nu alvast een idee van de stand van zaken met betrekking tot spambestrijding anno 2004. SpamAssassin kijkt namelijk naar de inhoud van e-mails en zoekt naar woorden als ‘sex’ of ‘viagra’. Naarmate dat soort woorden vaker voor komen in een e-mail, wordt de ‘spamscore’ steeds hoger. Zodra die score boven de 5.5 komt (op een schaal van 10), wordt de e-mail geweigerd. Om te voorkomen dat normale e-mail waar dit soort woorden in voorkomen per ongeluk ook wordt geweigerd, is het mogelijk om zelf te definiëren wanneer een e-mail spam is. In plaats van de grens bij 5.5 te leggen, is het ook mogelijk om die op bijvoorbeeld 6.5 in te stellen. Spammers proberen SpamAssassin te ontwijken door woorden te verbasteren (s3x, v1agr4). Tevens worden er ‘gewone’ woorden toegevoegd aan de e-mail, omdat die de

spamscore weer omlaag brengen. Dat dit leidt tot steeds minder leesbare e-mails mag blijken uit onderstaand voorbeeld (de volledige tekst van een spam e-mail gericht aan locuta@xs4all.nl, daterend van 8 maart 2004):

> *Our team of U.S. board-certified physicians and pharmacists provide you with professional medical advice and FDA-approved medications. Your choices: , v|aGR@ _ Pnter.m.in $ Va/l/ium ; X:A:Nax ~ S0ma > At|v.@n Plus: Fl3x'eril, Ce:|3brex, Fi0ric3:t, Tram@'do|, U|:tr@m, L3`v|tra, Pr0p3ci:a, Acyc`|0vir, Pr0z'@c, P@`xil, Busp:@r, Ad|`pex, I0nam*|n, M3ri`dia, X3nic.a|, Ambi.3n, S:0naTa We ship to almost Every Country in the World . No waiting rooms. Here. http://www.firstassist.biz. Throbs in my memory still: Let the dead Past bury its dead! The day is done, and the darkness Still, like muffled drums, are beating*

De combinatie in deze e-mail van medicijnen en poëzie mag dan best apart zijn, maar het zal voor de meeste mensen niet echt verhelderend werken. De poëzie althans, van de medicijnen weet ik het niet.

Waar spam meer dan twintig jaar geleden nog vanaf bestaande adressen werd verstuurd, soms met alle TO-adressen gewoon zichtbaar voor de ontvangers, is de methode van spammers langzamerhand steeds meer opgeschoven naar een technisch geraffineerd kat-en-muis spelletje met spambestrijders. Vervalste afzenderadressen, verminkte woorden, trucs om aan nieuwe e-mailadressen te komen, het hacken van pc's door middel van virussen om vervolgens vanuit die pc's te spammen, het zijn slechts enkele van de voorbeelden die genoemd kunnen worden in de evolutie van spam.

De meest voorkomende technieken van spammers om e-mails inhoudelijk te camoufleren zijn deze:

Black Hole

Verbergt tekst in een bericht door een ‘size-zero’ lettergrootte te gebruiken. De zichtbare tekst bestaat uit de oproep om product X te kopen, terwijl er daarnaast nog ettelijke regels onzichtbare tekst in de e-mail staan met gewone woorden, om spamfilters te ontwijken die gebruik maken van woordfiltering.

Numbers Game

Verbergt tekst voor filters door deze om te zetten in HTML codes of numerieke weergaven van speciale karakters.

Invisible Ink

Manipuleert tekst- en achtergrondkleur waardoor de tekst van e-mails letterlijk onzichtbaar is. Vergelijkbaar met de Black Hole methode.

Slice and Dice

Gebruikt HTML om een bericht in dunne stroken op te delen.

Content Encoding

Gebruikt standaard content codering om de echte inhoud van een e-mail te verbergen. De meest gebruikte coderingsvormen zijn Base64, BinHex en Quoted Printable.

Daily News

Voegt delen van teksten uit het nieuws in de tekst toe door middel van ‘invisible ink’ of aparte MIME-delen. MIME is een set afspraken die het mogelijk maakt om andere informatie dan platte tekst te verzenden en te ontvangen via internet.

Het camoufleren van de fysieke locatie van de spammer is echter het eerste waar de spammer zich zorgen om maakt. De methodes om ontdekking hiervan te voorkomen zijn eveneens vrij eenvoudig op te sommen.[25] De lijst is niet statisch, maar wordt zoals gezegd voortdurend aangepast door de continue strijd tussen spammers en spambestrijders:

Gebruik maken van inbelverbinding

Het eerste defensie mechanisme van een spammer is het gebruik maken van een inbelverbinding als hij zelf vanaf een eigen computer spamt. Bij gebruik van ADSL of een kabelverbinding is er meestal sprake van een vast IP-adres (Internet Protocol, de unieke numerieke code die wordt toegewezen aan een verbinding). Het is dan eenvoudig bij de provider waar dat IP-adres vandaan komt te achterhalen van wie dat IP-adres is en waar hij/zij woont. Bij een inbelverbinding wordt er echter een dynamisch IP-adres gegenereerd. Elke keer als er wordt ingebeld wordt er een ander IP-adres toegewezen. Dat maakt het al iets lastiger, maar de meeste internet providers kunnen ook dan de echte afzender meestal wel achterhalen. Tenminste, de fysieke locatie. Als die fysieke locatie echter een bibliotheek is bijvoorbeeld, dan loopt het spoor daar alsnog dood.

Gebruik maken van virussen

Een trojan horse is een bestand dat zich ongemerkt op de pc van een gebruiker nestelt en dat door een hacker gebruikt kan worden om verbinding te maken met weer een andere pc. Deze trojan/virus kan dan ‘naar huis bellen’ om spam te downloaden van vooraf bepaalde websites, die vervolgens automatisch vanuit de gehackte pc verder verstuurd wordt. De spammer is op deze manier niet te traceren. De lijn loopt dood bij de gebruiker van de gehackte pc. De trojan verspreidt zichzelf ondertussen verder naar andere slecht beveiligde internetgebruikers. En ook die verspreiden weer spam. De spammer hoeft ondertussen niets meer te doen dan achterover te zitten en af te wachten tot de bestellingen binnen stromen.

[25] In overleg met spamgoeroe Scott McIntyre, werkzaam als hoofd security/abuse bij de afdeling systeembeheer van internet provider XS4ALL.

Gebruik maken van open relay

Een open relay is een mailserver die mail van buiten zijn eigen domein accepteert en doorstuurt naar adressen buiten zijn eigen domein. Dat is niet de bedoeling, want zo'n mailserver kan door spammers misbruikt worden. De meeste internet providers scannen dan ook actief of hun klanten open relay draaien. Indien dat het geval is worden deze klanten direct afgesloten, totdat ze hun systemen weer juist geconfigureerd hebben. Spammers maken relatief veel gebruik van open relay.

Gebruik maken van open proxy

Breedbandabonnees met een ADSL- of kabelaansluiting willen vaak meerdere pc's aan elkaar koppelen in een netwerk. Er zijn programma's verkrijgbaar zoals Wingate of Winproxy die dit kunnen regelen. Indien deze programma's slecht geconfigureerd zijn, staan ze net als bij open relay open voor spammers. Open proxies komen steeds vaker voor.

Gebruik maken van scripts

Spammers zoeken naar websites die FormMail.pl en andere mail-a-form scripts hebben draaien die bedoeld zijn om via een website e-mail te sturen naar personen achter die website. Als deze verkeerd geconfigureerd zijn, is het voor buitenstaanders mogelijk om het script te gebruiken om e-mail naar allerlei adressen te versturen. Spammen is dan eenvoudig en de spammer is niet te achterhalen omdat de bron het mail-a-form lijkt te zijn.

Het kapen van een netblock

Sommige spammers maken gebruik van internet providers die zelf te weinig kennis hebben van de techniek achter internet. Spammers kunnen zo bijvoorbeeld aan een groep netwerk adressen komen die eigenlijk van iemand anders zijn. Daardoor

kunnen ze in relatief korte tijd heel veel spam versturen, totdat ze ontdekt en afgesloten worden. Dit is een soort alternatieve manier van het verschuilen achter een inbelverbinding.

Al deze ingenieuze methoden –en de vele obscure methoden die hier nog naast bestaan en waarschijnlijk op het moment van dit schrijven nog ontstaan- zorgen er in ieder geval voor dat er een voortdurende technologische strijd door en tegen spammers gevoerd wordt. Het is van belang om te weten hoe spam werkt om je een voorstelling te kunnen maken van de problematiek. En tevens om inzicht te krijgen in de mogelijke bestrijdingsmethodes, waar ik in een later hoofdstuk op terug kom.

2.3 Problemen met definitie

Waarom is spam een probleem? In het eerste hoofdstuk stipte ik deze vraag al aan. Hier zal ik hem uitgebreider proberen te beantwoorden. Ten eerste zijn er de kosten voor de ontvanger. Die zijn onevenredig hoog in vergelijking met de kosten van de verzender. De verzender kan met één druk op de knop miljoenen mensen bereiken. En een spammer is niet genoodzaakt om een sociaal optimale hoeveelheid e-mails te sturen, de kosten zijn immers niet voor de verzender maar voor de ontvanger. Elke ontvanger moet afzonderlijk de e-mail ophalen, lezen en verwijderen. Het tweede punt hangt hier direct mee samen: Internet Service Providers moeten extra e-mailservers plaatsen om de extra grote hoeveelheden e-mail te verwerken. Daarnaast betalen zij veel geld voor extra bandbreedte. Deze kosten kunnen eveneens alleen afgewenteld worden op de klanten, niet op de (onbekende) spammer. Het derde punt is de irritatie die spam bij de ontvanger oproept. Dit kan irritatie zijn vanwege de inhoud van de e-mail, maar het kan ook samenhangen met volgelopen mailboxen of lange wachttijden om de e-mail binnen te halen. Privacy is een vierde element in de problematisering van spam. Enerzijds kunnen ontvangers van spam zich afvragen hoe spammers aan hun adressen komen, anderzijds kunnen zij kwaad zijn over de ongewenste binnendringing in hun mailbox.

Spam blijkt dus duidelijk problemen te geven waarvan je echter zou verwachten dat ze eenvoudig op een juridische, technische, economische of communicatieve manier op te lossen zouden moeten zijn. Maar niets is minder waar. Effectieve bestrijding van spam vooronderstelt een eenduidige definitie van spam, maar die ontbreekt.

Eerder meldde ik dat twee belangrijke kenmerken van spam zijn:

- het ongevraagde c.q. ongewenste karakter
- de grootschalige verzending (bulk)

Maar hier zijn veel kanttekeningen bij te plaatsen. Internetproviders, consumenten(organisaties), bedrijfsleven, direct marketeers, overheden: iedereen hanteert een eigen definitie van spam. Vooral het gebrek aan consensus over de definitie van spam op juridisch gebied zorgt voor veel problemen.

De Organisatie voor Economische Samenwerking en Ontwikkeling (OECD) schrijft in haar recente 'background paper' over spam dat de moeilijkheid van een eenduidige definitie gelegen is in het feit dat er veel verschillende elementen in de definitie moeten worden opgenomen:

> *"A comprehensive definition might need to incorporate a diverse set of elements related to commercial behaviour, recipient psychology, the broader legal context, economic considerations, and technical issues."*[26]

[26] OECD (2004) Background paper

Dit is dan ook de belangrijkste reden dat er veel verschillende definities gehanteerd worden door diverse actoren. In definities over spam wordt meestal gesproken over kenmerken als bulk, commercieel, ongevraagd, het gebrek aan toestemming vooraf en de ongewenstheid van de boodschap. Maar ook het niet-discriminerende karakter (het enige wat bekend is van de ontvanger is het e-mailadres), de veelal vermomde afzender en de frauduleuze inhoud van berichten worden in definities opgenomen.

Een definitie die door veel Internet Service Providers (ISP's) wordt gebruikt is deze:

> *"Internet spam is one or more unsolicited messages, sent or posted as part of a larger collection of messages, all having substantially identical content."*[27]

Hier staan het ongevraagde karakter, het bulk element en de identieke context centraal. Opvallend is dat er in deze definitie geen onderscheid wordt gemaakt tussen commerciële en niet-commerciële berichten.

Een soortgelijke definitie wordt bijvoorbeeld gehanteerd door de Nederlandse ISP XS4ALL:

> *"Spam is het (massaal) versturen van ongevraagde berichten op internet met dezelfde boodschap, meestal met een commerciële inhoud, maar soms ook met een wervende politieke of charitatieve boodschap."*[28]

Hier wordt wel gesproken over het onderscheid tussen commerciële en niet-commerciële berichten, waarbij wordt gesteld dat spam zowel commercieel als niet-commercieel kan zijn.

---

[27] Monkeys (2003)
[28] XS4ALL Helpdesk (2001)

De meest gangbare definities van spam zijn echter: Unsolicited Bulk E-mail (UBE) en Unsolicited Commercial E-mail (UCE).[29]

Het enige kenmerk dat in vrijwel elke definitie van spam terugkomt is het ongevraagde element. De elementen 'bulk' en 'commercieel' uit voornoemde populaire definities zijn alleen relevant in combinatie met het ongevraagde karakter van de boodschap. Bulk alleen is niet voldoende, want een ontvanger van een spam e-mail weet niet aan hoeveel anderen het bericht nog meer wordt gestuurd en is daar ook niet in geïnteresseerd. Het gaat om toestemming, niet om kwantiteit. Dat een e-mail alleen maar spam is als er sprake is van een commerciële boodschap, is ook lastig vol te houden. Ook oproepen van charitatieve instellingen of politieke partijen kunnen als spam worden beschouwd.

Het is hierbij tevens interessant om stil te staan bij de vraag: 'spam volgens wie?' Zelfs als een wet zou zeggen dat niet-commerciële berichten niet onder de noemer spam vallen, dan nog kan de perceptie bij de ontvanger van het bericht heel anders zijn, wanneer die een andere definitie van spam hanteert waarbij niet het commerciële aspect een rol speelt, maar juist het ongevraagde karakter van een e-mail. De praktijksituatie wordt maar al te vaak uit het oog verloren bij spam. Want wat nu als 99% van de spam die een consument of bedrijf ontvangt uit charitatieve boodschappen zou bestaan in plaats van zoals nu uit commerciële boodschappen? Zou de (juridische) definitie van spam zich dan ook aanpassen aan die realiteit? Waarschijnlijk wel. Je ziet dan ook dat naarmate het soort spam in de loop der tijd verandert, ook de definities van spam mee veranderen. Tevens is er veel wet- en regelgeving die onderscheid maakt in verschillende soorten spam. Ook hier worden verschillende definities voor spam gehanteerd. Zo gelden er in Amerika andere regels voor het versturen van porno e-mails dan voor het aanprijzen van bijvoorbeeld vliegvakanties. In dat eerste geval is het niet slechts het ongevraagde karakter van de e-mails dat van belang is, maar gaat het ook om de bescherming van kinderen ('*Spam messages containing pornographic photographs,and promoting adult entertainment products and services are deemd inappropriate for*

[29] Sorkin, David E. (2001)

children.') en werknemers (*'Under US Law, it is clear that pornographic email leaves companies vulnerable to charges of creating 'a hostile work environment', and all the associated liabilities that implies.'*).[30]

Het Instituut voor Informatierecht (IViR) van de Universiteit van Amsterdam heeft de wet- en regelgeving op spamgebied op Europees niveau het afgelopen jaar onderzocht. Ook zij concluderen dat de kern van spam het ongevraagde karakter betreft. De definitie van spam die zij in hun onderzoek hanteren is *'unsolicited communications for direct marketing purposes'*. [31]

Ik zelf sluit mij aan bij de eerder genoemde definitie die o.a. XS4ALL hanteert:

> *'Spam is het (massaal) versturen van ongevraagde berichten op internet met dezelfde boodschap, meestal met een commerciële inhoud, maar soms ook met een wervende politieke of charitatieve boodschap.'*

Ik kies voor deze definitie omdat het een aantal van de belangrijkste elementen die in de verschillende definities van spam genoemd worden in zich heeft: het massale karakter, het ongevraagde element, het -voor mijn scriptie relevante-

[30] IviR (2004), Blz. 63
[31] IviR (2004), Blz. 12

Justitie straft computercriminelen

DEN HAAG - Minister Donner van Justitie gaat het inbreken en platleggen van computernetwerken te lijf. Mensen die zich aan een dergelijk computervergrijp schuldig maken, hangt een celstraf van maximaal een jaar boven het hoofd.

Iedereen die grote hoeveelheden spam (ongewenste e-mail) stuurt met als doel computersystemen te ontregelen of zelfs plat te leggen, wordt strafrechtelijk vervolgd. Dat geldt ook voor mensen die computervirussen versturen.

Volgens Donner wordt niet alle spam strafbaar. Reclame e-mail zal niet worden aangepakt. De Tweede Kamer heeft daar vorig jaar wel op aangedrongen.

Bron: NOS Teletekst, 2 maart 2004

aspect van het aan internet gerelateerd zijn en tenslotte de afweging tussen commerciële en niet-commerciële berichten, die in deze definitie beide onder de noemer spam kunnen vallen.

Los van de juridische problemen bij de definitie van spam zijn er ook veel communicatie problemen.

Het is vervelend dat er geen eensluidende wereldwijd geaccepteerde juridische definitie is van spam, maar ook in de media en zelfs binnen overheidsorganisaties wordt voor veel onduidelijkheid gezorgd als het gaat om de vraag wat spam nu precies is. In het teletekst bericht dat hiernaast afgebeeld staat is hier een mooi voorbeeld van te zien. Daarin wordt ten eerste gesproken over het versturen van grote hoeveelheden spam met als doel computersystemen te ontregelen. Het doel van het versturen van grote hoeveelheden spam is echter niet het ontregelen van systemen, maar het verkopen van diensten en producten. Dat door die grote hoeveelheden spam computersystemen ontregeld worden, is geen doel van spam, maar een negatief gevolg. Ten tweede eindigt het bericht met de opmerking van Donner dat niet alle spam strafbaar wordt: “Reclame e-mail zal niet worden aangepakt.” Maar laat spam nu juist reclame e-mail zijn...

De verwarring komt van twee kanten. Enerzijds quote NOS Teletekst Donner in die laatste regels op een onvolledige manier –hetgeen onvermijdelijk is door de korte lengte van teletekstberichten waardoor belangrijke informatie verloren kan gaan-, anderzijds heeft Donner wel degelijk gezegd dat spam met als doel het ontregelen van computersystemen strafrechtelijke vervolging op zal leveren.[32]

[32] Ministerie van Justitie, persbericht 3 maart 2004

2.4 Conclusie

Om spam te kunnen bestrijden is het noodzakelijk om te weten hoe e-mail precies werkt en hoe het technische proces achter spam precies in elkaar steekt. Het blijkt heel eenvoudig te zijn om spam te versturen. Een computer met een internetaansluiting is al voldoende.

De bestrijding van spam is erg lastig. Er is namelijk geen eenduidige definitie van spam. Alle betrokken actoren zoals consumenten, overheden en bedrijfsleven hanteren verschillende definities van het begrip spam. Een deel van de verklaring van de definitieproblemen ligt verscholen in de veelheid aan elementen die in de definitie zou moeten worden opgenomen. Een ander deel van de verklaring draait om de verschillende percepties die actoren hanteren bij spam. Zij hebben verschillende belangen bij spam: de ontvanger van spam wil er niets mee te maken hebben, de verzender ziet het juist als zijn broodwinning. Het enige kenmerk dat in vrijwel elke definitie naar voren komt is het ongevraagde karakter van de communicatie.

Hoofdstuk 3
Methoden van spambestrijding

Inleiding

Naast de problemen met de definitie van spam, zijn er ook problemen bij de daadwerkelijke bestrijding van spam. Waarom hebben we nog steeds last van spam? Wat wordt er eigenlijk gedaan om spam te bestrijden? Deze laatste vraag zal centraal staan in dit hoofdstuk. Achtereenvolgens komen de technische, economische, juridische en communicatieve aanpak aan bod. Daarna volgt nog een stukje over de (on)mogelijkheden van zelfregulering, waarna ik afsluit met de effectiviteit van alle methoden en hun eventuele beperkingen.

3.1 Technische aanpak

De meest gebruikte praktische maatregel om spam te bestrijden is een technische aanpak. De meeste internetproviders bieden technische spamfilters aan die zoveel mogelijk ongewenste e-mails buiten de deur moeten houden. Internetters kunnen indien zij dat willen ook zelf een technisch filter aanbrengen. Er zijn veel manieren om spamfilters te creëren. De meest gebruikte zullen hier worden behandeld, te weten:

- Basic structured text filters
- Content based filters (Bayesian filters)

- Spamassassin
- Honeypotting
- DNS Blocklists
- Client-side filtering
- Blacklists / Whitelists

Er zijn natuurlijk nog veel meer vormen van technische filtering en er worden ook dagelijks nieuwe methoden uitgevonden of verfijnd. Maar bovenstaande opties zijn verreweg de meest populaire en effectieve maatregelen. Met name SpamAssassin wordt wereldwijd in allerlei vormen ingezet om spam te bestrijden.

1. Basic structured text filters (client-side filtering)

De meeste e-mailprogramma's hebben de mogelijkheid om e-mail te sorteren op basis van teksten die worden gevonden in de headers en body van de e-mail. Het e-mailprogramma kijkt dan of bepaalde woorden of woordcombinaties in de e-mail voorkomen en bepaald aan de hand daarvan of een e-mail spam is of niet. Bij deze methode is het risico op 'false positives' echter groot. Dat zijn e-mails die geen spam zijn, maar toch als zodanig worden beschouwd en verwijderd. Client-side spam filters zijn specifiek bedoeld voor de uiteindelijke ontvanger van de e-mail. Dit in tegenstelling tot server-side filtering waarbij de internet provider probeert de spam weg te filteren. Sommige e-mailprogramma's bevatten de optie om 'fake bounce messages' te sturen. De verzender krijgt dan bericht dat het adres waaraan werd geprobeerd het bericht af te leveren niet zou bestaan. Maar deze optie is in de meeste gevallen volstrekt zinloos: er is waarschijnlijk geen spammer die het afzender adres niet vervalst heeft. Door het sturen van het bounce bericht wordt alleen de internet provider extra belast die deze boodschap moet verwerken.

2. Content based filters (Bayesian filters)

Bayesian filters berekenen op basis van de inhoud van een bericht de waarschijnlijkheid dat een bericht spam is. Het verschil met basic structured text filters is dat het Bayesian filter kan leren. Het filter zoekt naar woorden uit de e-mail die typerend zijn voor spam en geeft deze een score. Ook de headers van de e-mail worden doorgelicht. Voor typische spamkarakteristieken krijgt de e-mail een hogere score, als er ook woorden in voorkomen die typerend zijn voor gewone e-mails dan wordt de score weer lager. De totale score is dan bijvoorbeeld 5. Bij een Bayesian filter kan de gebruiker meestal zelf aangeven boven welke score een e-mail als spam moet worden beschouwd. Bijvoorbeeld boven de zes. Alleen die e-mails worden dan gefilterd.[33]

Er zijn een aantal problemen met deze manier van filteren. Voordat het programma voldoende geleerd heeft om tot accurate beoordelingen te komen moeten er honderden e-mails gescand zijn. Daarnaast zijn de karakteristieken waarop wordt gezocht vastgelegd. Een spammer die weet dat het filter zoekt naar ‘viagra’ kan dit simpelweg omzeilen door van het woord ‘viiagra’ te maken. En ook bij deze filtertechniek is de kans op false positives weer groot.

3. SpamAssassin

SpamAssassin maakt gebruik van de techniek van Bayesian filters. Maar daarnaast voert het nog extra checks uit, zoals header tests, het aanmaken van automatisch white- of blacklists en het gebruik maken van DNS-blocklists. SpamAssassin probeert samengevat een aantal filtertechnieken te combineren om tot de best mogelijke identificatie van spam te komen. En niet alleen inkomende e-mail kan

[33] Tschabitscher, Heinz (2004)

gecontroleerd worden, maar ook uitgaande e-mail. Op deze manier kan worden gemonitord of er niet een virus actief is op een pc die spam probeert te verspreiden.

Een groot voordeel is dat SpamAssassin erg dynamisch is. Het is mogelijk om zelf allerlei soorten filtering uit of aan te zetten. Ondanks de combinatie van technieken zijn er ook bij SpamAssassin echter nog veel false positives en false negatives. Die laatste categorie bevat e-mails die onterecht niet als spam zijn aangemerkt.

4. Honeypotting

Honeypotting is een techniek die door met name hele grote providers en aanbieders van e-mailadressen wordt gebruikt. Providers kunnen bij bedrijven als Brightmail, Postini of Messagelabs lijsten met honeypots inkopen. De naam zegt het al: er wordt gewerkt met lokkertjes voor spammers. Op de lijsten staan tot wel honderden miljoenen adressen die niet in gebruik zijn van gewone klanten. Elke e-mail aan deze adressen is per definitie ongevraagd en wordt dus als spam gekwalificeerd. De adressen fungeren als 'spamtraps'; de afzenders kunnen meteen worden toegevoegd aan blacklists. Het aantal false positives is bij goed gebruik van honeypots laag. Er kan bijvoorbeeld aangegeven worden dat de e-mail op minstens één miljoen van de 100 miljoen adressen aangekomen moet zijn voordat het definitief als spam wordt aangemerkt. Pas dan wordt de e-mail voor alle klanten van de provider die van deze spamfiltering gebruik maken geweigerd. Een probleem is echter dat honeypots vaak te laat echt werken. Op het moment dat een e-mail als spam geclassificeerd is, kan de e-mail al op vele duizenden gewone adressen afgeleverd zijn.

Alleen indien de spammer in een later stadium nóg een spam e-mail stuurt vanaf hetzelfde adres of vanaf dezelfde machine is de honeypot echt effectief. De e-mail wordt dan direct geweigerd voor alle klanten. De meeste spammers gebruiken echter zelden twee keer achter elkaar dezelfde machine of hetzelfde adres om te spammen.

Een ander nadeel van honeypotting is dat de licentiekosten van dergelijke software over het algemeen gebaseerd zijn op het aantal e-mail adressen waarop gefilterd moet worden. Providers die deze software afnemen, zullen deze kosten dus vaak één op één doorberekenen aan hun klanten.[34]

5. DNS Blocklists

DNS blocklists kijken alleen naar het IP-adres van de verzendende machine. Ze bevatten lijsten die criteria bevatten op basis waarvan e-mail gefilterd kan worden door internet providers. De meest gebruikte blocklists zijn blocklists met puur technische of juist gemengde criteria, boycot-blocklists en blocklists gebaseerd op (ongecontroleerde) meldingen door het internetpubliek in het algemeen. De lijsten verschillen in de mate van betrouwbaarheid; bij sommige lijsten is de kans minimaal dat legitieme e-mail als spam wordt aangemerkt, bij andere lijsten is de kans heel groot dat een grote provider als Hotmail of AOL tijdelijk wordt geblokkeerd.[35]

Blocklists met puur technische criteria nemen een IP-adres op in hun database als deze voldoet aan bepaalde technische eigenschappen die veel misbruikt worden voor het versturen van spam.

Boycot-blocklists bevatten IP-adressen die toebehoren aan onverbeterlijke spammers. Het gebruik van een boycotlijst om e-mail te weigeren helpt zeer effectief bij het bestrijden van spam. Het doel van dergelijke lists is het massaal weigeren van e-mail van een domein of provider, om daarmee de providers van spammers onder druk te zetten. Een groot nadeel is dat ook de legitieme e-mail van alle klanten van een provider hierdoor geweigerd kunnen worden. Bij de laatste categorie DNS-blocklists kunnen klanten van providers

[34] Nas, Sjoera (2002)
[35] XS4ALL (2002)

zelf spam rapporteren bij Spamcop (www.spamcop.net). Bij vijf rapportages van verschillende klanten wordt een afzender dan al op de blacklist gezet. Een kwaadwillende kan op deze manier iemand tot spammer verklaren, terwijl hij dat niet is.

Over het algemeen werken DNS blocklists heel goed, maar de gevaren zijn duidelijk. DNS blocklists worden dan ook steeds vaker (slechts) als onderdeel van SpamAssassin gebruikt.

6. Blacklists / Whitelists

Blacklists en whitelists werden al eerder genoemd. Een blacklist is een ‘zwarte lijst’ waarop de adressen worden bijgehouden die beschouwd worden als spamadressen. Meestal worden dit soort lijsten client-side beheerd. Op een whitelist staan juist de adressen die de ontvanger ongeacht de inhoud van het bericht door wil laten. Dit ‘trusted sender’ principe kent een groot nadeel: het vereist een extra handeling van de persoon die een e-mail probeert te sturen. Die krijgt namelijk een automatisch gegenereerd bericht met het verzoek om bijvoorbeeld een bepaald woord in te tikken op een website zodat de ontvanger zeker weet dat hij met een mens van vlees en bloed te doen heeft. Dit hoeft slechts eenmalig, maar als iemand een legitieme e-maillijst heeft met duizenden mensen die ineens allemaal met whitelists gaan werken, dan is het beheren van zo’n lijst ineens ondoenlijk. Ook blacklists hebben een groot nadeel: het aantal false negatives is erg hoog, omdat spammers hun afzenderadres keer op keer wijzigen.

3.2 Economische aanpak

Een discussie die regelmatig wordt gevoerd op met name het internet zelf gaat over het bestrijden van het spamprobleem door een economische aanpak. Door spammers direct in hun portemonnee te treffen zou het probleem opgelost kunnen worden. Er zijn een

aantal suggesties gedaan om deze economische aanpak te effectueren. Maar meer dan dat is het nooit geworden, vanwege de vele haken en ogen die aan zo'n aanpak zouden zitten. Toch blijft de discussie telkens weer oplaaien, dus het behandelen van de voornaamste methoden op economisch gebied is wel relevant.

Er zijn maar twee methoden om spammers direct in hun portemonnee te treffen:

- Micropayments (digitale postzegels)
- Boetes

Micropayments

Bij het gebruik van micropayments oftewel digitale postzegels (E-stamps) betaalt de verzender van een e-mail voor elk verzonden bericht een klein bedrag, bijvoorbeeld 0,01 eurocent. Net als bij gewone post zouden mensen dan moeten gaan betalen voor het verzenden van berichten. Het voordeel van het versturen van digitale berichten is dat het in principe niet uitmaakt hoe groot een bericht is (hoe dik de virtuele envelop is), voor elk bericht kan in principe eenzelfde bedrag gehanteerd worden.

De grootste kracht van dit systeem volgens de voorstanders is dat het normale verzenders van e-mails slechts beperkt belast. Als een internetgebruiker 50 berichten per dag verstuurt dan zou dat maar 0,50 eurocent kosten. Spammers daarentegen worden hard getroffen. Die verzenden hun e-mails in de regel naar honderdduizenden of miljoenen adressen. Voor hen zouden de kosten dan te hoog worden om spam nog economisch rendabel te laten zijn.[36]

[36] Templeton, Brad (2004) E-stamps

De nadelen van het systeem zijn echter legio. Ten eerste moeten zowel de verzender als de ontvanger aan het systeem meedoen. De verzender moet een digitale postzegel plakken (en heeft dus een e-mailprogramma nodig waarin dat mogelijk is) en de ontvanger moet een e-mailprogramma hebben dat de digitale postzegel herkend. Ten tweede zijn legitieme mailers met grote maillijsten de dupe van dit systeem: zij hebben soms wel tienduizenden klanten die hebben aangegeven wel interesse te hebben in bepaalde mailings, maar ook daarvoor moet de verzender dan betalen. Ten derde zou het hele idee van internet als gratis, openbaar, wereldwijd communicatiemedium ten gronde gaan als er voor elke e-mail betaald zou moeten worden. Ten vierde is er een online geldstransfersysteem nodig, zijn er nieuwe e-mailprogramma's noodzakelijk die met digitale postzegels om kunnen gaan. Dat is een gigantische operatie die tot dusverre niet ondernomen is.

En een van de belangrijkste redenen waarom digitale postzegels ongewenst zijn is dat de meeste spam verstuurd wordt via gehackte pc's. Als een spammer een pc hackt en vervolgens vanaf die pc de spam laat versturen, dan gaat de rekening voor de digitale postzegels naar de gebruiker van die pc en niet naar de spammer. En de spam komt gewoon aan bij alle ontvangers, want er zit dan immers netjes een postzegel op het bericht.

Er zijn varianten op het micropaymentsysteem,. Zo kun je de ontvanger laten kiezen of de verzender wel of geen postzegel moet betalen. Bij ontvangst klikt hij op een knop die de keuze bepaalt of er wel of niet betaald moet worden. Bij een 'nee' zou dan alle nieuwe e-mail van die verzender voortaan gratis geaccepteerd kunnen worden. Dit zou dan een vorm van whitelisting zijn. Maar ook dit vereist veel handelingen en kan wrevel oproepen bij de verzender die er wellicht van uit gaat dat de e-mail zonder postzegel wordt toegelaten. Al deze nadelen gecombineerd hebben er toe geleid dat micropayments nooit een echt serieuze optie zijn geweest om spam te bestrijden.

Boetes

Boetes zijn de tweede economische optie om spammers aan te pakken. Dit hangt nauw samen met de juridische bestrijdingsmaatregelen, bestaande uit wet- en regelgeving. Zodra een spammer gepakt is kan hij beboet worden. In de meeste landen waar een vorm van een spamverbod bestaat worden spammers inderdaad beboet. In Nederland kan die boete oplopen tot 4.500 euro.

Het grote praktische probleem bij het uitdelen van boetes is echter dat er nauwelijks spammers gepakt worden. In Nederland zijn bijvoorbeelds slechts enkele boetes uitgedeeld.[37] Spammers zijn dan ook nauwelijks te traceren. De Nederlandse wetgeving (voortkomend uit een Europese richtlijn) voorziet alleen in de aanpak van Nederlandse spammers, maar de meeste spam komt juist van over de grens. De onlangs door toezichthouder OPTA ingestelde website spamklacht.nl waar 'particuliere eindgebruikers' kunnen klagen over spam uit alleen Nederland heeft dan ook niet veel meer dan een symbolische functie. En zelfs de nog recentere gebundelde aanpak van een dertiental Europese landen is nog veel te vrijblijvend (vrijwillige samenwerking) en territoriaal (slechts 13 landen) en inhoudelijk (informatie uitwisseling) beperkt om meer dan een deuk in een pakje boter te slaan.[38]
Het is niet alleen een probleem om spammers te traceren, maar zolang de spam wordt verzonden via landen waar spammen niet verboden is dan werken boetes sowieso niet meer. Elk land zou dus in principe mee moeten doen aan dit boetesysteem. Ook boetes lijken dus niet de oplossing van het spamprobleem te zijn.

[37] Eind december maakte het Ministerie van Economische Zaken bekend dat er boetes uitgedeeld zijn aan twee ondernemingen en een persoon. Zie voor het bericht www.ez.nl/content.jsp?objectid=28950. Overigens heeft een van de beboete spammers inmiddels al bezwaar aangetekend en bij de Tweede Kamer geklaagd over de OPTA omdat deze er dubieuze praktijken op zou nahouden bij de handhaving van het verbod op het versturen van ongevraagde e-mail aan consumenten (zie www.webwereld.nl/nieuws/21191.phtml).
[38] In februari kondigde een dertiental Europese landen aan om informatie over spam te delen met de toezichthoudende instanties in die landen. Eurocommissaris Reding gaf echter direct al toe dat de meeste spam van buiten de EU afkomstig is. Zie www.webwereld.nl/nieuws/20733.phtml

3.3 Juridische aanpak

Naast technische methoden om spam te bestrijden zijn wet- en regelgeving de meest gebruikte manieren om spammers een halt toe te roepen. De ontwikkelingen op dat gebied gaan hard. Wet- en regelgeving wordt steeds verder verfijnd. Als voorbeeld van het voortschrijdend inzicht bij wet- en regelgeving en de gevolgen daarvan volgt hieronder in vogelvlucht het verloop van de ontwikkelingen in Europese wet- en regelgeving sinds 1995. Ook de rol van de Nederlandse overheid wordt hierbij belicht. Aparte aandacht is er voor de VS, één van de landen waar de meeste spam vandaan komt.

3.3.1 Wet- en regelgeving in de Europese Unie

1995: Algemene Privacy richtlijn

In 1995 werden algemene regels voor het verwerken van persoonsgegevens vastgesteld in de Algemene Privacy Richtlijn.[39] Deze richtlijn heeft niet rechtstreeks betrekking op spam, maar e-mailadressen kunnen wel worden gezien als persoonsgegevens. In artikel 6 van de richtlijn wordt het doelbeginsel uitgelegd. Dit houdt in dat persoonsgegevens slechts verwerkt mogen worden indien zij voor specifieke, uitdrukkelijk omschreven doeleinden zijn verkregen en overeenkomstig deze doelen eerlijk worden verwerkt. In de praktijk komt het er voor spambestrijding op neer dat het verzamelen van e-mailadressen aan regels wordt gebonden. Zomaar op internet e-mailadressen verzamelen mag niet meer. Daarnaast is er een informatieplicht van de verantwoordelijke jegens de betrokkene

[39] Richtlijn 95/46/EC

(overweging 47 uit de richtlijn). De verantwoordelijke wordt verplicht om zijn identiteit, doeleinden en verdere informatie die nodig is om een eerlijke verwerking te waarborgen kenbaar te maken aan de betrokkene.

1997: Richtlijn Overeenkomsten op Afstand

De Richtlijn Overeenkomsten op Afstand[40] uit 1997 is de eerste richtlijn die consumenten probeert te beschermen tegen ongewenste communicatie. De richtlijn vereist voorafgaande toestemming van de consument indien er gebruik wordt gemaakt van 'automated calling systems without human intervention and fax as a means of distance communication for the conclusion of a contract between consumer and supplier'.[41] Andere manieren van communicatie zijn alleen toegestaan indien er vooraf goedkeuring is verleend door de consument.[42] Dit laatste kan dan van toepassing zijn op e-mail. Maar wederom is de richtlijn niet specifiek opgesteld voor e-mail. Daarnaast is de richtlijn opgesteld ter bescherming van consumenten, niet van bedrijven en andere instellingen.

1997: ISDN Richtlijn

Eveneens in 1997 verscheen de ISDN Richtlijn[43] die feitelijk slechts een aanvulling was op de Algemene Privacy Richtlijn uit 1995. Naast de verwerking van persoonsgegevens wordt hierin ook de persoonlijke levenssfeer beschermd. Deze bescherming beperkt zich echter tot de telecommunicatiesector. De kern van de richtlijn is terug te vinden in artikel 12 en is tweeledig. Ten eerste kan het gebruik maken van de eerdergenoemde automated calling systems alleen worden toegestaan als er vooraf goedkeuring is verleend door de

[40] Richtlijn 97/7/EC
[41] Richtlijn 97/7/EC, art. 101
[42] Richtlijn 97/7/EC, art. 10.2
[43] Richtlijn 97/66/EC

consument (zie Richtlijn Overeenkomsten op Afstand) en ten tweede wordt aan lidstaten de keuze gelaten of ze dit willen handhaven door middel van een opt-in of een opt-out regime. Nederland koos in dit geval voor het opt-out regime.

2000: Richtlijn Elektronische Handel

In de Richtlijn Elektronische Handel[44] wordt voor het eerst expliciet melding gemaakt van e-mail als een voorbeeld van ongewenste communicatie. Artikel 6 van de richtlijn stelt dat commerciële communicatie ten minste als zodanig herkenbaar moet zijn en dat de afzender duidelijk herkenbaar moet zijn. Indien een lidstaat voor het opt-out regime gekozen heeft moeten verzenders van commerciële boodschappen volgens lid 7 van het artikel regelmatig de meest recente opt-out lijsten raadplegen. Wat 'regelmatig' precies is en wie die opt-out lijsten dan bij zou moeten houden werd in de richtlijn niet duidelijk gemaakt. Het belangrijkste minpunt is echter het feit dat de richtlijn beperkt is tot alleen commerciële communicatie.

2002: E-privacy Richtlijn

Ter vervanging van de ISDN Richtlijn verscheen in 2000 de E-privacy Richtlijn.[45] Deze richtlijn maakte onderdeel uit van een vijftal telecommunicatie richtlijnen die moeten zorgen voor één interne Europese markt voor de media en telecommunicatiesector. Ongeacht de technologieën waar gebruik van werd gemaakt wordt gepoogd de bescherming van persoonsgegevens in de telecommunicatiesector te waarborgen. Wat nieuw is in de richtlijn is dat e-mail expliciet is opgenomen in de lijst van verplichte opt-in:

[44] Richtlijn 2000/31/EC
[45] Richtlijn 2002/58/EC

'The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) ***or electronic mail*** *for the purpose of direct marketing may only be allowed in respect of subscribers who have given their prior consent.'*[46]

Het betreft echter alleen direct marketing e-mails. Direct marketing wordt niet gedefinieerd in de richtlijn. Commerciële spam, UCE, wordt door middel van deze richtlijn verboden, met één uitzondering: Indien er sprake is van een bestaande klantrelatie, dan mag commerciële e-mail wel ongevraagd worden toegestuurd.

De reikwijdte van de richtlijnen

De Europese regelgeving biedt uitgaande van de genoemde richtlijnen vooral bescherming tegen commerciële e-mail. Door de onduidelijkheid over de uitleg en naleving van de bepalingen, alsmede door de keuze tussen verschillende systemen waar lidstaten voor konden opteren (opt-in versus opt-out) is uiteindelijk de E-privacy richtlijn tot stand gekomen waar in beginsel sprake is van het opt-in systeem.

Op 19 mei 2004 werd de Telecommunicatiewet in Nederland van kracht, waar de E-privacy richtlijn in was omgezet. De kritiek van met name internet providers en bedrijven was dat alleen consumenten tegen spam beschermd worden. Als handhaver van het spamverbod is de OPTA aangewezen. Internetters kunnen daar op basis van artikel 11.7 van de Telecommunicatiewet terecht met hun spamklachten via de speciaal daar voor opgezette website www.spamklacht.nl. Maar zoals eerder gezegd kunnen daar alleen 'particuliere eindgebruikers' hun klachten kwijt over spam uit alleen Nederland.[47]

[46] Richtlijn 2002/58/EC, art. 13
[47] Zie bijlage B

Daarnaast zijn er een paar belangrijke mazen in de wet. In februari 2004 bepaalde de rechtbank in Amsterdam dat een e-mailbestand uit een faillissement mocht worden doorverkocht aan een derde partij.[48] De ‘bestaande klantrelatie’ ging hierbij over op de nieuwe eigenaar die vervolgens gebruik mocht maken van het e-mailbestand om daar zijn eigen (commerciële) boodschappen heen te sturen. Een ander lek is het feit dat alleen berichten met een commercieel, ideëel of charitatief karakter onder het verbod op spam vallen. Indien iemand 100.000 e-mails met zijn of haar vakantiefoto’s doorstuurt, dan is dat gewoon toegestaan.

Een lek met een positieve lading werd door de Hoge Raad vastgesteld in haar uitspraak van 13 maart 2004. De Raad besliste dat internetprovider XS4ALL spam mag weigeren op haar netwerk. De uitspraak was de uiteindelijke conclusie op de rechtszaak die XS4ALL in 2002 had aangespannen tegen AbFab, een bedrijf dat ongevraagde e-mails verstuurde, onder andere naar klanten van XS4ALL. De Hoge Raad vindt het feit "dat XS4ALL exclusieve rechten heeft op haar computercapaciteit, transmissiecapaciteit en klantenbestand (haar computersysteem)" veel zwaarder wegen dan het beroep op vrijheid van meningsuiting dat Abfab deed. Heel algemeen stelt de HR: Een provider heeft dus geen vervoersplicht. Op grond van dit arrest kunnen alle providers in Nederland op voorhand een verbod eisen op het toezenden van spam, ook als dit aan hun zakelijke klanten is gericht. Daarmee gaat dit oordeel verder dan de Europese richtlijn.[49]

[48] LJN: AO3649, KG 04/65 SR (2004)
[49] NLIP (2004)

3.3.2 Wet- en regelgeving in de Verenigde Staten

In de Verenigde Staten wordt spam niet simpelweg als een inbreuk op de privacy gezien zoals in Europa. Vanaf de eerste klachten werd spam in de Verenigde Staten gezien als overlast gevend en als een vorm van huisvredebreuk.[50]

In 2001 waren er achttien staten die wet- en regelgeving op het gebied van spam hadden, waarbij sommige spam verboden en andere juist expliciet toestemming gaven om ongewenste e-mails te versturen. Het duurde tot 2004 voordat er wetgeving kwam die boven de federale staten uitsteeg. In januari 2004 trad de 'Controlling the Assault of Non-Solicited Pornography and Marketing Act' (CAN-SPAM) in werking.[51] De kern van CAN-SPAM is dat bedrijven ongevraagd commerciële e-mail mogen sturen, zolang ze maar een opt-out mogelijkheid bieden. Deze wet is dus het tegenovergestelde van de Europese wet- en regelgeving die juist het opt-in principe heeft omarmd. Het gaat dus om het verschil tussen 'ja, mits' en 'nee, tenzij'.

Een ander nadeel is dat sommige Amerikaanse staten anti-spam maatregelen hadden die verder gingen dan CAN-SPAM. Die maatregelen zijn nu 'overruled'.

3.3.3. Effecten van juridische maatregelen

Is er nu minder spam door juridische maatregelen? Nee, de bestaande wet- en regelgeving voldoet in geen enkel land. Ondanks de vrijwel overal toegenomen wettelijke maatregelen tegen spam is het aantal spam e-mails niet verminderd. Alleen toen in de Verenigde

[50] Hawley, Anne E. (1997)
[51] United States Congress (2003)

Staten de CAN-SPAM-act in werking trad was daar een korte dip te zien in de spamcijfers, die kort daarna echter weer op het oude niveau terugkeerden.[52] Toch is de hoop van veel spambestrijders op wet- en regelgeving gericht. Dat de mazen in de wet nu vrijwel overal nog zo groot zijn als het gat in de ozonlaag betekent niet dat er in het geheel geen ontwikkeling in zit. Wet- en regelgeving wordt als noodzakelijk gezien om spambestrijding effectief te laten zijn, maar niet als wondermiddel. Het is één van de instrumenten waarmee spambestrijding mogelijk is. Twee voorbeelden:

De brancheorganisatie van Nederlandse Internet Providers (NLIP) ziet voorlichting aan internetgebruikers over het beveiligen van hun systemen als een ander belangrijk hulpmiddel.

> *'Spammers maken namelijk op grote schaal gebruik van slecht beveiligde computers van gewone internetgebruikers (de zogenaamde open proxies). Echter, de branche en de internetgebruikers kunnen het niet alleen. Het treffen van preventieve maatregelen heeft weinig effect als het spamverbod niet effectief wordt gehandhaafd. Het is daarom cruciaal dat overheden stevig optreden als blijkt dat bedrijven de wet overtreden en toch ongevraagde mail versturen.'*[53]

En minister Brinkhorst ziet ook een combinatie van wet- en regelgeving en andere maatregelen als oplossing.

> *'De strijd tegen ongewenste e-mails (spam) moet vooral worden gewonnen door technische oplossingen. Wetten alleen zijn niet genoeg, zo heeft minister Brinkhorst (Economische Zaken) maandag verklaard na overleg met zijn EU-collega's.'*[54]

[52] Verhagen, Laurens (2004) Antispammaatregelen VS nog weinig effectief, en ANP (2004)
[53] NLIP (2004)
[54] Ministerie van Economische Zaken, persbericht 9 maart 2004

Voor ‘gewone’ bedrijven, instellingen en personen is wet- en regelgeving wel degelijk relevant. Al is het maar voor het rechtvaardigheidsgevoel van de ontvanger van spam. Maar ook op de verzenders van spam heeft wet- en regelgeving invloed. Bedrijven als KPN of de Rabobank zullen zich aan de regels houden, daar alleen al de schade aan hun imago gigantisch zou zijn wanneer zij zouden gaan spammen. Maar de echte spammers zijn meestal ronduit crimineel en hebben geen boodschap aan een slecht imago. Wet- en regelgeving heeft daar nauwelijks invloed op. Hooguit zal een spammer overwegen de spam vanuit een land te versturen waar spammen nog niet verboden is. Zolang nog niet elk land op de planeet sluitende wet- en regelgeving heeft, zijn juridische maatregelen slechts een druppel op een gloeiende plaat, om over handhaving nog maar te zwijgen. Grensoverschrijdende samenwerkingsverbanden tussen politie- en justitie-instanties bestaan vrijwel nergens. Het verzamelen van bewijs en het oppakken en vervolgen van een betrapte spammer gebeurt dan ook nog nergens. Daarnaast valt de E-privacy richtlijn in Italië bijvoorbeeld onder het strafrecht waardoor gevangenisstraf mogelijk wordt indien er gespamd wordt, maar in Nederland onder het bestuursrecht, waardoor slechts boetes als sanctie kunnen worden opgelegd.

En ten slotte loopt in veel landen niet alleen de wet- en regelgeving sterk uiteen, maar ook de opvattingen over spambestrijding als het gaat om voorlichting. Zo adviseert de OPTA op https://www.spamklacht.nl/asp/overspam/doentegenspam.asp#2 om niet op unsubscribe-links te klikken. Volgens de amerikaanse CAN-SPAM-wetgeving zijn dergelijke links juist verplicht, in het daar gehanteerde opt-out systeem. In dit voorbeeld is het overigens de OPTA die het juiste advies geeft: bij de meeste spam e-mails wordt een gebruiker juist op nieuwe spamlijsten gezet als hij op een unsubscribe-link klikt, daar de spammer dan weet dat het e-mailadres kennelijk echt in gebruik en dus waardevol is.

3.4 Communicatieve aanpak

Een methode van spambestrijding die echt nog in de kinderschoenen staat is de communicatieve aanpak. Het gaat dan over preventie van spam door middel van voorlichting. In de internetwereld wordt ook wel gesproken over het creëren van ‘user-awareness’.

Zo kan een voorlichtingsactie er voor zorgen dat spam (tijdelijk) wordt gereduceerd of zelfs voorkomen wordt. De belangrijkste praktische tips die hierbij gegeven zouden kunnen worden zijn deze:

- Neem een e-mailadres dat niet al te eenvoudig is. Dictionary attacks die lukraak woord- en cijfercombinaties uitproberen zullen een adres als john@hotmail.com snel vinden. john.johnson@hotmail.com is alweer een stuk lastiger.
- Zet een e-mailadres niet overal op internet. Spamrobots die daar e-mailadressen oogsten door alles te verzamelen waar een @ in voorkomt kunnen een adres dan snel te pakken krijgen.
- Gebruik nooit een echt e-mailadres op nieuwsgroepen. Als spamrobots ergens actief zijn op het internet, dan is het wel in nieuwsgroepen. En het archief van deze nieuwsgroepen blijft eeuwig online staan. Als er slechts één keer vanaf een bepaald e-mailadres iets verstuurd is naar een nieuwsgroep, dan is de kans bijna 100% dat een spammer dat adres te pakken krijgt. Een veelgebruikte oplossing is om in het e-mailadres de woorden NO.SPAM te zetten. De lezer van het adres moet dan zelf die letters uit het e-mailadres verwijderen. Bijvoorbeeld: john.johnsonNO.SPAM@hotmail.com. Een nadeel is dat de lezer dit wel moet snappen.
- Geef geen antwoord op spam e-mails, ze komen vrijwel nooit aan, daar de verzender het afzender adres in de regel vervalst heeft. Antwoorden op spam e-mails belasten slechts de internet provider die een antwoord weer door moet sturen.
- Klik nooit op unsubscribe-links in spam e-mails. De spammer weet dan dat het e-mailadres in gebruik is en zal het adres op nog meer spamlijsten toevoegen.

- Open nooit attachments in e-mails waarvan de afzender of de inhoud onbekend is. In 99% van de gevallen gaat het om virussen. Dat is op zich al erg genoeg, maar spammers gebruiken virussen steeds vaker om vanuit een besmette pc spam e-mails te versturen.

Een nadeel van voorlichting als spambestrijdingsmiddel is dat het louter preventief werkt. Voorlichting is een bijzonder kostbare aangelegenheid waarvan niemand de kosten graag wil dragen. In de praktijk zijn het nu vaak internetproviders en internetgebruikers die proberen om gebruikers voor te lichten, maar het is de vraag of ook overheden hier niet een rol in zouden moeten spelen. Nu internet en met name e-mail bijna een nutsvoorziening zijn geworden in veel landen kun je je afvragen of er niet sprake is van een algemeen publiek belang dat beschermd zou moeten worden door de overheid. Die (politieke) keuze is in de meeste landen nog niet gemaakt. In Nederland heeft minister Brinkhorst van Economische Zaken daar in maart een uitspraak over gedaan. "Ask not what your country can do for you, but what you can do for your country", zo citeerde hij John F. Kennedy.[55] Hij is dan ook voorstander van een marktoplossing: 'De strijd tegen ongewenste e-mails moet vooral worden gewonnen door technische oplossingen. Wetten alleen zijn niet genoeg.'[56]

Dat er ook bij de overheid soms sprake kan zijn van voortschrijdend inzicht bewijst dezelfde minister Brinkhorst op 27 oktober 2004. In een reactie op kamervragen van het CDA meent Brinkhorst dat veel internetgebruikers niet doorhebben dat hun computer wordt misbruikt voor het versturen van spam.[57]

[55] Bits of Freedom (2004)
[56] Ministerie van Economische Zaken, persbericht 9 maart 2004
[57] Reijnders, Maarten (2004)

"Om gebruikers van internet meer bewust te laten worden van de kwetsbaarheid van hun systeem voor deze praktijken en de risico's die zij daarbij lopen is een goede voorlichting van groot belang. Internetgebruikers moeten ertoe gebracht worden hun pc afdoende te beveiligen. Juist over praktijken als het creëren van zombie-netwerken, maar ook bijvoorbeeld over spoofing en phishing zal meer voorlichting worden gegeven."

De minister heeft inmiddels Europese subsidie aangevraagd voor de voorlichtingsactie ‘Surf op Safe’.

3.5 Zelfregulering

Zelfregulering is gemeengoed voor de advertentie industrie.[58] De kracht van zelfregulering is dat het aansluit bij de praktijk, de werkprocessen en keuzes van de doelgroep. Maar de economische en politieke en juridische rationaliteit staan hier echter tegenover elkaar. De wettelijke kaders waarbinnen zelfregulering plaats kan vinden zijn heel belangrijk. Als de kwaliteit daarvan goed is, kan de overheid op hoofdlijnen sturen. Wetten bieden in dat geval de ruimte voor checks en balances. Hoe ruimer die wetten blijven, hoe meer dat de goedkeuring van voorstanders van zelfregulering wegdraagt.

Ook als het om spam gaat proberen brancheorganisaties door middel van zelfregulering al te stringente wet- en regelgeving te voorkomen. In de meeste gevallen wordt er voorgesteld om opt-out lijsten op te stellen waar aangesloten bedrijven gebruik van kunnen maken. Door de E-privacy richtlijn is dat in de Europese Unie echter niet meer mogelijk, daar het opt-in systeem voor commerciële boodschappen wordt gehanteerd. In Nederland was de verwarring over de complexe regelgeving zelfs compleet toen de Stichting

[58] Baggott, Rob en Harrison, Larry (1986)

Reclame Code op 15 juni 2004 de Code Verspreiding Reclame via E-mail in werking stelde.[59] Kern van de Code is dat er geen e-mailreclame naar een persoon mag worden gestuurd als deze daar niet om heeft gevraagd. Dit sluit in principe naadloos aan op de E-privacy richtlijn. De grote 'blunder' is echter dat de Code over personen spreekt.

> *'Hoewel de direct marketing branche de intentie had om een code te schrijven gericht op consumenten, lijkt zij zich verkeken te hebben op het brede kader van de Reclame Code. Op basis van de e-mail code kunnen nu ook personen met een zakelijk e-mailadres klachten indienen bij de Reclame Code Commissie. De direct marketing branche geeft hierdoor zakelijke e-mailadressen bescherming terwijl men daartegen succesvol gelobbied heeft bij de behandeling van de Telecommunicatiewet.'*[60]

Het belangrijke punt waarop zelfregulering faalt is echter dat de meeste spammers niet lid zijn van dit soort brancheorganisaties. Specifieker: zelfregulering is niet mogelijk omdat er dan sprake zou moeten zijn van een kenbaar aantal leden in een branche en dat is bij spam niet het geval.[61] Iedereen met een internetverbinding kan spammen. Overigens proberen internetgebruikers soms zelf spammers dwars te zitten. Een ludiek voorbeeld is Spampoison. Internetters wordt gevraagd naar een pagina te linken zodat de robot van de spammer er naartoe getrokken wordt wanneer deze de pagina doorzoekt.

[59] Reclame Code Commissie (2004)
[60] Bits of Freedom (2004)
[61] Elburg, Anton van (2003)

'Robots die e-mailadressen verzamelen zullen in een eindeloze lus terechtkomen en dynamisch gegenereerde valse e-mailadressen ophalen, waardoor ze enorme hoeveelheden gefingeerde gegevens aan de gegevensbestanden van de spammers toevoegen en die zodanig vervuilen dat ze feitelijk onbruikbaar worden.' [62]

Dit zou je ook een poging tot een vorm van zelfregulering (van het internet) kunnen noemen.

3.6 Conclusie

Geen enkele van de genoemde spambestrijdings methoden lost het spamprobleem op. Technische filters hebben allemaal hun beperkingen en kunnen soms zelfs internet providers in de problemen brengen waarvan alle klanten door te strenge spamfilters van andere providers worden geblokkeerd. Economische oplossingen bestaan vrijwel alleen op papier, juridische maatregelen staan nog in de kinderschoenen en hebben vaak nauwelijks invloed op de 'criminele' spammers die juist verantwoordelijk zijn voor het afleveren van de meeste spam. Daarnaast zijn juridische maatregelen vaak niet of nauwelijks grensoverschrijdend, wat juist noodzakelijk is omdat spam dat ook is. Communicatieve maatregelen zijn eveneens nog vrij nieuw en bieden hoe dan ook geen oplossing voor mensen die inmiddels al overspoeld worden door spam. En aan zelfregulering doen notoire spammers niet mee.

In het volgende hoofdstuk zal ik dan ook dieper ingaan op de vraag hoe het komt dat de huidige methoden niet voldoen. Wat is de theoretische achtergrond die kan helpen om dit te verklaren?

[62] Spampoison (2004)

Hoofdstuk 4
Theoretisch kader

When you take stuff from one writer it's plagiarism;
But when you take it from many writers, it's research.
Wilson Mizner (1876-1933)

In dit hoofdstuk gaan we even terug in de tijd: wat is er veranderd in de maatschappij en welke gevolgen heeft dat gehad voor het oplossen van (complexe) vraagstukken? Wat zijn nu de theoretische handvatten om een antwoord te kunnen geven op de vraag: 'hoe manage je een netwerk?'

4.1 Heel de aarde is mijn vaderland

Vroeger was alles beter, hoor je oudere mensen regelmatig verzuchten. Het waarheidsgehalte van die uitspraak is moeilijk te toetsen, maar het lijkt er soms wel op dat veel zaken vroeger wat eenvoudiger waren. Sturing geven aan de maatschappij bijvoorbeeld. Tegen het einde van de 19e eeuw was de Nederlandse overheid nog klein wat betreft het aantal ambtenaren, er was een heldere scheiding tussen publieke en private taken, de ministeriële verantwoordelijkheid was duidelijk vastgelegd en de overheid kende een duidelijke hiërarchie (het primaat van de politiek) en had een beperkte taakstelling. Om maatschappelijke vraagstukken op te lossen was kennisverwerving (en het op basis van die kennis formuleren van oplossingen) dé aanpak om sturing te geven aan de maatschappij.[63]

[63] Kingdon, J.W. (1984)

Het leek toen allemaal een simpele kwestie van doelen stellen, taken afbakenen en het implementeren van het nieuwe beleid. De organisatie van de vereiste handhaving van nieuwe wetgeving was relatief eenvoudig: het was helder welke instantie in welk gebied jurisdictie had.

In de twintigste eeuw veranderde de samenleving echter snel. Eerst door de reeds eind 19e eeuw ingezette industriële revolutie, die onder andere massaproductie mogelijk maakte en zorgde voor een razendsnelle uitbreiding van vervoersmogelijkheden om die producten te verspreiden. In de laatste decennia van de twintigste eeuw volgde de informatie revolutie, ook wel ICT-revolutie genoemd, omdat die twee zo onlosmakelijk met elkaar verbonden waren. De ontwikkelingen op ICT-gebied volgden elkaar in razend tempo op. Tussen de eerste grote mainframes die bijna letterlijk huizenhoog waren en de pocket pc's die we nu kennen zit amper een halve eeuw. Het internet waar in 1991 een handjevol techneuten mee bezig was, is in veel landen inmiddels bijna een nutsvoorziening geworden. De ICT-ontwikkelingen van de afgelopen decennia hebben hiermee grote gevolgen voor de samenleving gehad.

In 1998 probeerde in Nederland de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in een toekomstverkenning de nieuwe mogelijkheden en obstakels uiteen te zetten die deze ICT-ontwikkelingen met zich mee zouden kunnen brengen. In het rapport, getiteld 'Staat zonder land', is deterritorialisering het centrale begrip. De WRR stelt dat door ICT-ontwikkelingen begrippen als 'afstand' en 'tijd' een wezenlijk andere rol gaan spelen. Veel activiteiten kunnen dankzij ICT wereldwijd worden ontplooid, onafhankelijk van de geografische locatie. Deterritorialisering wordt door de WRR gedefinieerd als een verdergaande vorm van internationalisering, waarvan sprake is indien menselijke activiteiten of interacties tussen mensen zich niet meer eenduidig laten toeschrijven aan een specifiek en daarbij passend rechtsregime.[64] De afnemende binding aan een bepaald grondgebied heeft volgens het rapport 'onvermijdelijke gevolgen voor het handelingsvermogen van de nationale staat', door de gebondenheid van instrumenten aan territoriale grenzen. Zo is

[64] WRR (1998) Blz. 9 en 54

wet- en regelgeving onlosmakelijk aan territoir gebonden. Door internationalisering krijgen burgers en bedrijven meer mogelijkheden om het beleid en de (rechts)verplichtingen van de nationale staat te ontlopen of te ontduiken. Indien staten proberen een begunstigend beleid voor de nationale markt proberen te voeren om zo juist een positieve impuls aan het nationale beleid te geven, kunnen daar echter ook actoren van elders van profiteren. [65] Door al deze zaken wordt de soevereiniteit van de nationale staten uitgedaagd en wordt uiteindelijk het handelingsvermogen van deze staten uitgehold.[66] Deterritorialisering is hiermee niet alleen een instrumenteel probleem, maar heeft ook alles te maken met legitimiteit.

Wat spam betreft, blijkt vrijwel de hele wereld erg voordelig te zijn om daar de activiteiten te laten neerslaan; grensoverschrijdende wetgeving is er immers niet of nauwelijks. Zo ontlopen en ontduiken spammers inderdaad het beleid. Ze maken gebruik (of misbruik) van de technologische ontwikkelingen op ICT-gebied. Ze zijn inderdaad onafhankelijk van een geografische locatie om hun activiteiten te ontplooien. Slechts een computer en een internet aansluiting zijn voldoende om de (internet)wereld op haar grondvesten te doen schudden. En er is meer dan spam alleen dat hier aan mee helpt. ICT gerelateerde issues die qua problematiek sterk op die van spam lijken zijn virusbestrijding, auteursrecht en privacy. In vrijwel al deze gevallen blijkt deterritorialisering voor wetgevings- en handhavingsproblemen te zorgen.

Internet

Het internet biedt hiermee misschien wel de beste voorbeelden van grensoverschrijdende activiteiten die gevolgen hebben voor het handelingsvermogen van nationale staten. Het internet heeft geen hiërarchisch karakter. Er is geen ‘baas’ van het internet. Actoren zitten letterlijk in een (inter)netwerk waar feitelijk het recht van de sterkste of de slimste geldt. Het internet bestaat uit een losse

[65] WRR (1998) Blz. 53
[66] Derksen, W.J. ‘De vage grenzen van de democratie’

aaneenschakeling van miljoenen computers die met elkaar communiceren door middel van het TCP/IP protocol, een universele taal bestaande uit het Transmission Control Protocol (TCP) en het Internet Protocol (IP). Er is geen supercomputer, persoon of instantie die eigenaar is van het internet, of die het internet kan controleren. Het opvragen van digitale gegevens van een computer in een ander land (grensoverschrijdend) is een net zo eenvoudige handeling als het halen van een brood bij de bakker. Ware het niet dat voor dat laatste nog een fysieke verplaatsing nodig is, die bij het gebruik van internet al overbodig is. Door de platte structuur van het internet is het makkelijk om informatie te versturen en te ontvangen. Maar tegelijkertijd kan er ook misbruik gemaakt worden van de technologische onvolkomenheden die het internet eveneens kenmerken. Om maar een paar voorbeelden te noemen: computers kunnen gehackt worden, systemen zijn ontvankelijk voor DOS-attacks (Denial Of Service), waarbij een dusdanig grote hoeveelheid informatie wordt opgevraagd van een systeem dat dit systeem crasht (Denial Of Service), en spammers kunnen vrijuit e-mails versturen die niet gewenst zijn. Er is niemand die als eindverantwoordelijke voor het internet de macht heeft om dit soort zaken te verbieden. En serieuze grensoverschrijdende pogingen hiertoe zijn er nog steeds niet.

De hoeveelheid spam is de laatste jaren dan ook alleen maar toegenomen. Het spambestrijdingsbeleid lijkt in veel landen op niet veel meer dan een pavlovreactie. Van een eventuele nieuwe vorm van functioneel bestuur dat de territoriale grenzen overschrijdt en dit soort problemen effectief aan kan pakken, is nog geen sprake.

4.2 Netwerken

De hypothese die uitgaande van deze grensoverschrijdende spamproblematiek gesteld kan worden, is dat maatregelen om spam te bestrijden net als spam zelf grensoverschrijdend zou moeten zijn om effectief te kunnen zijn. Het is nu bijvoorbeeld onduidelijk onder welk rechtsregime een Nederlandse spammer valt die in de Verenigde Staten achter zijn computer zit om te spammen, terwijl die spam

via machines in Zuid-Korea wordt verstuurd naar gebruikers in Australië. Spam overschrijdt bestaande territoriale grenzen en dat heeft gevolgen voor het handelingsvermogen van nationale staten. Zij zijn immers instrumenteel gebonden aan territoriale grenzen en bij spam is die binding tussen handeling en territoir er niet.

Door de toegenomen complexiteit van maatschappelijke vraagstukken is het zelfstandig oplossen van dit soort problemen in steeds mindere mate mogelijk, constateerde Glasbergen al in 1989.[67] Samenwerking tussen nationale staten lijkt derhalve onvermijdelijk om tot een oplossing van het spamprobleem te komen. In Nederland kan de overheid spam wel verbieden, maar het dilemma is -zoals zojuist geschetst werd- dat spam vaak niet uit Nederland zelf komt, maar uit een ander land. Waarbij het dus ook nog eens lastig aan te geven is uit welk land dan precies. In dit soort situaties is de Nederlandse overheid slechts een onderdeel in een netwerk van actoren, bij spam bijvoorbeeld bestaande uit andere overheden, internet providers, gebruikers, bedrijfsleven, etc. Op de meeste beleidsterreinen is de overheid nog steeds gezaghebbend en weet zij sturing te geven aan de maatschappij, maar niet op alle gebieden lukt het de overheid om als centrale actor greep te houden op ontwikkelingen in de samenleving. Spam blijkt hier een goed voorbeeld van te zijn. Niets gaat immers zo makkelijk over territoriale grenzen heen als digitale informatie.

De Nederlandse overheid bevindt zich dus in een internationaal netwerk als het gaat om spambestrijding. En het gaat dan niet alleen om wet- en regelgeving als methode van spambestrijding, maar ook over andere methoden. Niet alleen overheden zijn onderdeel van het spambestrijdingsspel, maar ook talloze internetproviders, gebruikers, bedrijven en zelfs spammers. Al deze actoren hebben eigen belangen en ideeën over oplossingen van het spamprobleem. Hoe is het nu mogelijk om tot een succesvolle oplossing te komen in zo'n netwerk? Om hier een antwoord op te kunnen geven is het noodzakelijk om te bekijken wat de netwerkbenadering precies inhoudt

[67] Glasbergen, P. (1989)

en welke voorwaarden er door deze benadering worden gesteld om tot een succesvolle manier te komen waarop dit soort beleidsprocessen benaderd moeten worden.

4.2.1. De netwerkbenadering

Volgens de netwerkbenadering staat in netwerken interactie tussen actoren en hun doeleinden centraal, in plaats van dat er uit wordt gegaan van één centrale actor. Top-down sturing vanuit de overheid kan in de meeste netwerksituaties niet langer, omdat er vaak geen sprake van een top meer is. In plaats daarvan is er sprake van wederzijdse afhankelijkheden tussen actoren waardoor de mogelijkheden tot hiërarchische sturing beperkt worden.[68] Sturing vindt plaats in complexe beleidsnetwerken, die te definiëren zijn als relatief stabiele patronen van sociale relaties tussen wederzijds afhankelijke actoren, die zich vormen rondom beleidsproblemen of clusters van middelen en die gevormd en in stand gehouden worden door een reeks van spelen.[69] Actoren zijn in netwerken wederzijds van elkaar afhankelijk in het komen tot oplossingen voor hun problemen. Daar alle actoren een eigen probleemperceptie en eigen doelen en uitgangspunten hebben, moeten zij de andere actoren in het netwerk ervan overtuigen dat hun visie juist is. Er moet een gezamenlijk referentiekader worden ontwikkeld waarin consensus kan worden bereikt over de te nemen stappen om doelen te kunnen bereiken. Er worden in netwerken dan ook vaak (tijdelijke) coalities gesloten om de eigen doelen (deels) te kunnen bereiken. Die samenwerkingsverbanden komen echter veelal niet spontaan tot stand. Daarvoor is netwerkmanagement noodzakelijk. [70]

[68] Kickert, W.J.M. (1985)
[69] Kickert, W.J.M., E.H. Klijn and J.F.M. Koppenjan (1997)
[70] Klijn, E.H. & J.F.M. Koppenjan (1997) Blz. 148

Bij het geven van een omschrijving van een netwerk is er sprake van drie veel terugkerende kenmerken, te weten pluriformiteit, geslotenheid en interdependentie.[71] Om kosten te delen en risico's te spreiden delen ondernemingen en soms ook overheden hun kennis. Dit creëert *wederzijdse afhankelijkheden* en zorgt voor een *toenemende verstrengeling* van die kennis. Pluriformiteit manifesteert zich op meerdere niveaus: niet alleen verschillen de betrokken actoren in het netwerk van elkaar wat betreft hun doelen, belangen en percepties, zij kunnen zelfs intern van mening verschillen, waardoor er dan sprake kan zijn van onderlinge concurrentie. *Geslotenheid van actoren* wil zeggen dat men in verschillende organisaties, instellingen en/of culturen dusdanig van het eigen gelijk overtuigd kan zijn, dat cognitieve fixatie optreedt. Dit is een vorm van groepsdenken waarin nieuwe informatie wordt genegeerd of wordt omgebogen naar eigen inzicht. Informatie uit de eigen organisatie wordt sneller opgepikt dan informatie van buitenaf.

Maar dit is geen uitputtende lijst.[72] En er zijn ook andere factoren die een rol spelen bij het ontstaan en de werking van netwerken, waarvan kennis van een aantal van deze factoren van belang is om het spamprobleem op te kunnen lossen. *Globalisering* zorgt voor grensoverschrijdende activiteiten, die eveneens wederzijdse afhankelijkheden creëren. *Deterritorialisering* staat in het verlengde hiervan voor een afnemende binding met een geografische locatie, waardoor het onduidelijk is onder wel rechtsregime een handeling valt. Er ontstaan ook steeds meer *horizontale relaties*. Actoren laten zich niet meer zomaar de wet voorschrijven, maar eisen (meer) invloed in besluitvormingsprocessen. Hierdoor staat soms niet langer wet- en regelgeving centraal, maar juist overleg. Dit benadrukt en creëert wederom de wederzijdse afhankelijkheden die nadrukkelijk centraal blijken te staan in een netwerk. Het gezagshebbende karakter dat zo kenmerkend is voor een hiërarchisch gestructureerde maatschappij of organisatie verdwijnt langzamerhand op een aantal punten. *Onzekerheid* ten slotte heeft betrekking op het niet weten wat de belangen, percepties en doelen van andere actoren zijn. Zolang de onzekerheid daarover te groot is, zal samenwerking niet of slecht tot stand komen. Het reduceren van onzekerheden is dus van belang om tot een vruchtbare samenwerking te komen.

[71] De Bruijn, J.A., Ten Heuvelhof, E.F. (1995) Blz. 9
[72] Klijn, E.H. & J.F.M. Koppenjan (2004) Blz. 4 en Bruijn, J.A. de & E.F. ten Heuvelhof (1995) Blz. 9

Beleidsprocessen kunnen derhalve worden gezien als complexe spelen tussen actoren. Al die actoren hebben elk hun eigen perceptie over de aard van het probleem, de gewenste oplossingen en de andere actoren in het netwerk. Op basis van die percepties kiezen de actoren een strategie. Succes of falen van het spel worden bepaald door de interacties van strategieën van de betrokken actoren. [73]

4.2.2 Globalisering en deterritorialisering

Globalisering en deterritorialisering beschrijven het ontstaan van (wereldwijde) netwerken. Daar spam grensoverschrijdend is, verdienen met name deterritorialisering en globalisering extra aandacht. Waar globalisering er voor zorgde dat grenzen (soms letterlijk) vervaagden, stelde deterritorialisering in het verlengde hiervan dat bepaalde activiteiten niet meer aan een specifiek rechtsregime toe te schrijven waren. Het handelingsvermogen van nationale staten nam hierdoor af. Door het vervagen van grenzen is niet alleen het transport van fysieke producten makkelijker geworden, maar ook het vervoer van kennis en informatie is dankzij ICT-ontwikkelingen veel eenvoudiger en goedkoper geworden. Helaas maken deze ICT-ontwikkelingen misbruik van het systeem ook mogelijk, waar spam zoals eerder geconstateerd een mooi voorbeeld van is.

Globalisering

Er is steeds meer wereldwijde samenwerking op economisch gebied, zoals bedrijven die op globale schaal gaan opereren. Ook op sociaal gebied worden er steeds meer onderlinge verbanden gelegd tussen reeds lang bestaande en nieuwe organisaties. Zo kunnen bijvoorbeeld geïnteresseerden in stedelijke hoogbouw elkaar vinden op forums of congressen die dankzij de steeds verder afnemende

[73] Klijn, E.H. & J.F.M. Koppenjan (1997) Blz. 149

kosten van transport, uitgedrukt in zowel tijd als geld, wereldwijd gehouden kunnen worden. Ook op politiek gebied worden grenzen geslecht. De uitbreiding van de Europese Unie is hier een goed voorbeeld van, waarbij bevoegdheden die eerst alleen aan de nationale staat werden toegewezen nu worden overgeheveld naar een supranationale autoriteit. Ook nationale staten zoeken elkaar dus steeds meer op. Op cultureel gebied is eveneens sprake van internationalisering. Zo lijkt de West-Europese cultuur in veel opzichten verbazingwekkend op die van de Verenigde Staten. Denk bijvoorbeeld maar aan muziek, films en eetcultuur.

Eigenlijk is er bijna geen onderwerp meer te bedenken dat niet grensoverschrijdend is. Als de OPEC de olieprijzen verhoogt, dan voelen wij dat in onze portemonnee wanneer we de auto bij moeten tanken. Steeds meer onderwerpen houden zich van nature ook niet (meer) aan door de mens vastgestelde grenzen. Een vervuilde rivier stopt niet met stromen bij de grensovergang naar een ander land. En ook spam wordt niet door een digitaal hek tegengehouden zodra de postbode de oceaan over moet. En dat globalisering soms letterlijk een vlucht neemt blijkt uit de noodzaak om wereldwijd afspraken te maken tussen vluchtleidingen over het luchtruim, omdat botsingen tussen vliegtuigen anders nauwelijks te vermijden zijn.

Globalisering kenmerkt zich grofweg door de volgende vier elementen:[74]

Uitgebreid sociaal netwerk: Er zijn wereldwijd nieuwe culturele, economische en politieke verbindingsnetwerken ontstaan. Gebeurtenissen en beslissingen aan de ene kant van de wereld hebben hierdoor invloed op de andere kant van de wereld.

[74] Held, D. (2000) Blz. 22

Intensivering van relaties: De toegenomen sociale contacten zijn geïntensiveerd. Staten raken meer betrokken met de wereld om zich heen. Door moderne communicatiemiddelen raken we in contact met andere gebieden in de wereld die daardoor dichterbij komen. De gevolgen en impact van gebeurtenissen voelen we hierdoor sterker dan ooit tevoren.

Toenemende onderlinge beïnvloeding: Door bovengenoemde punten komen verschillende culturen met elkaar in contact. Zij beïnvloeden elkaar en nemen elkaars gebruiken en gewoonten over. Denk bijvoorbeeld aan Hollywood films die wereldwijd verspreid worden.

Mondiale infrastructuur: Netwerken handelen buiten de nationale staten om. Ze hebben hun eigen infrastructuur die grenzen overschrijdt.

Door deze globalisering, of 'grensoverschrijdende activiteiten die in omvang, intensiteit, invloed en snelheid van deze wereldwijde onderlinge verbondenheid variëren', ontstaan steeds meer wederzijdse afhankelijkheden.[75] Het is onmogelijk om als nationale staat onafhankelijk van de rest van de wereld te blijven bestaan. Geen enkel land is zelfvoorzienend, ook al zouden de Verenigde Staten dat bijvoorbeeld graag willen zijn. Maar zelfs zij, of juist zij, zijn afhankelijk van de hulp van andere landen en uiteindelijk ook van organisaties als de Verenigde Naties die wel een breedgedragen mandaat hebben waardoor bepaalde doelen makkelijker bereikt kunnen worden. Terrorismebestrijding is een 'mooi' voorbeeld van een grensoverschrijdende activiteit waarbij wederzijdse afhankelijkheden ervoor zorgen dat eenzijdige actie geen oplossing biedt. Er hoeft maar een uitleveringsverdrag met één land te ontbreken en een terrorist kan al niet meer gepakt worden.

[75] Held, D. (2000) Blz. 24

Deterritorialisering

In de inleiding van dit hoofdstuk sprak ik al over deterritorialisering en de hiermee samenhangende onvermijdelijke gevolgen voor het handelingsvermogen van de nationale staat. Deterritorialisering hangt nauw samen met de afname van de macht (en daarmee invloed) van de nationale staat als het gaat om ict-ontwikkelingen die het mogelijk maken voor actoren om zich aan bestaande rechtsregimes te onttrekken.

Het internet daagt het idee van territorium op drie manieren uit:[76]

1 - Geografische grenzen spelen geen rol van betekenis meer. Informatievoorziening kan los van bestaande bestuurlijke patronen worden georganiseerd, los van het domein van een organisatie. Verbindingen en koppelingen kunnen worden aangebracht op elk moment en tussen elk gewenst niveau van besluitvorming.[77] Ook hier komt de vraag dus naar voren hoe het zit met het primaat van de politiek. Het vervagen van grenzen heeft tot gevolg dat ook de uitoefening van dit primaat onder druk komt te staan. De WRR sprak zei hier het volgende over in het rapport 'Staat zonder land':[78]

> *"Plaats en afstand worden steeds minder belangrijk. Waar in de fysieke wereld doorgaans een drie-eenheid bestaat van actor, actie en gevolg op dezelfde plaats, kan ICT ertoe leiden dat deze drie-eenheid gefragmenteerd wordt. De actor zit bijvoorbeeld ergens achter een toetsenbord en verricht een handeling op afstand, waardoor op weer een andere plaats effect ontstaat."*

[76] Bekkers, V.J.J.M. (1998)
[77] Frissen, P.H.A. (1996)
[78] WRR (1998) Blz. 44

2- Geografie en gemeenschapsvorming worden ontkoppeld. Virtuele gemeenschappen en digitale steden ontstaan.

3- Gevolgen voor geografische deconcentratie van overheidsvoorzieningen. De toegankelijkheid tot overheidsvoorzieningen krijgt door internet een nieuwe dimensie. Veel zaken kunnen online worden afgehandeld. Het virtuele loket rukt op.
Deterritorialisering leidt niet alleen tot praktische problemen (en overigens soms ook juist oplossingen voor reeds bestaande problemen!) met betrekking tot handhaving, maar ook tot problemen van meer principiële aard. De WRR zegt hierover:

> *'Dit geldt in het bijzonder voor de juridische kernfunctie van de staat, het monopolie op het stellen en handhaven van bindende regels, welke sterk gebaseerd is op de feitelijke notie dat actor, actie en gevolg aan een en dezelfde plaats zijn te verbinden. (...) Het feit dat betrokkenen zelf lokaliseerbaar kunnen zijn, doet aan dit probleem niet af, zolang wet- en regelgeving zo zeer uitgaat van het territorialiteitsbeginsel.'*[79]

Bij spam is het probleem vaak nog een graad erger. Niet alleen is het onduidelijk onder welk rechtsregime een spammer zou vallen als hij fysiek op een andere locatie is dan waar de e-mail vandaan lijkt te komen (en ook terecht komt op weer een andere locatie), maar het is vaak zelfs helemaal niet mogelijk om de spammer te lokaliseren. Het internet biedt uitgebreide mogelijkheden om de geografische locatie van een internetter te maskeren. Nog ingewikkelder wordt het zelfs wanneer spammers gebruik maken van virussen om hun spam mee te verzenden vanaf besmette pc's. Wie is er dan aansprakelijk te stellen? De eigenaar van de besmette pc die immers de spam daadwerkelijk verzendt, degene die het virus heeft geschreven? De internet provider die de virussen per e-mail door laat sturen? Microsoft of Apple die hun systemen kennelijk niet voldoende weten te beveiligen tegen virussen? De gebruiker die

[79] WRR (1998) Blz. 8 en 55

zijn pc niet goed beschermd heeft tegen virusbesmettingen? Of wellicht toch de spammer die van het virus gebruik maakte om zijn ongewenste e-mails mee rond te sturen? Dit zijn de vragen waar spambestrijders nu een antwoord op proberen te formuleren.

4.3 Effectiviteit van de netwerkbenadering

Wanneer kan het gebruik maken van de netwerkbenadering nu effectief zijn? Aan welke voorwaarden moet worden voldaan om tot een succesvolle benadering van het beleidsproces te komen? Sturing in (virtuele) netwerken blijkt erg lastig te zijn. In situaties waarin de overheid niet meer zomaar sturing kan geven aan de maatschappij op basis van een hiërarchisch, centraal aangestuurd model, zijn logische vragen: hoe dan wel? Is de overheid slechts één van de spelers, of is er toch een onderscheid met andere actoren? Moet de overheid wel willen sturen op dit soort terreinen? Een aantal antwoorden is wel te geven. De nationale staat mag dan niet langer op alle terreinen de machts- en gezaghebbende structuur binnen het publieke domein zijn, maar ze heeft wel het geweldsmonopolie en is –in de meeste gevallen- democratisch gelegitimeerd. De overheid heeft het monopolie voor de gezaghebbende toedeling van waarden en op basis daarvan dient zij publieke belangen te waarborgen. Het waarborgen van een goed functionerend e-mail systeem lijkt zo'n publiek belang te zijn. E-mail is een belangrijke manier van communicatie geworden op zowel sociaal (privé-berichten) als economisch (zakelijk e-mailverkeer) vlak. En deze vorm van communicatie wordt door spam steeds meer belemmerd, waarbij -zoals we in hoofdstuk 1 al zagen- zowel de economische als sociale kosten steeds verder toenemen.

Om te voorkomen dat het machtsevenwicht verschuift naar plaatsen buiten de overheid, die niet democratisch gelegitimeerd zijn, is een tegenoffensief noodzakelijk om complexe problemen in netwerken te verdisconteren. Volgens Frissen ligt een belangrijke nieuwe taak voor de politiek daarom in het nadenken over hoe in een archipel-achtige (virtueel) rijk van organisaties en samenwerkingsrelaties

patronen van verantwoording en democratische controle ingericht kunnen worden.[80] Daarbij zou volgens hem afgestapt moeten worden van het klassieke idee dat verantwoording en controle altijd een hiërarchisch patroon hebben. Het probleem van deze opvatting is echter dat het geen antwoord geeft op de vraag waar gezaghebbende waarden in de maatschappij toegedeeld zouden moeten worden. En afstappen van het hiërarchische patroon van verantwoording en controle klinkt wel interessant (en noodzakelijk omdat het in de praktijk simpelweg niet altijd meer werkt?), maar hoe die nieuwe vorm van controle en verantwoording er dan wel uit moet zien, dat is onduidelijk en het debat daarover staat helaas niet zoals Frissen zou willen op de politieke agenda.

De gecreëerde of soms simpelweg spontaan ontstane netwerken zorgen dus ook voor nieuwe problematiek en de aanpak daarvan vereist nieuwe sturingsmechanismen. En het is dus de vraag hoe je in een netwerk waarin niet of nauwelijks sprake is van hiërarchische verhoudingen vorm kunt geven aan die sturing. Wat de rol van overheden dan is of kan zijn, kan pas bepaald worden als duidelijk is welke sturingsvormen er mogelijk zijn in netwerken. Daar moet dus eerst verder naar gekeken worden. De eerste generatie sturingsinstrumenten (communicatieve, economische en juridische instrumenten) zijn eenzijdig, top-down en direct en dat werkt nu juist niet in een netwerk. De tweede generatie instrumenten (meerzijdige instrumenten, persoonsgerichte instrumenten, incentives, kengetallen, etc.) is beter geschikt in netwerksituaties. Zij houden beter rekening met de geslotenheid, pluriformiteit en interdependentie van actoren in het netwerk. Maar om überhaupt aan het inzetten van instrumenten toe te komen is het eerst noodzakelijk dat er samenwerking ontstaat gericht op een gezamenlijke oplossing van maatschappelijke problemen. De sturing faalt al direct als er geen voorwaarden voor samenwerking zijn, of als er blokkades zijn (of blijven bestaan) voor interactie.

De noodzakelijke voorwaarden voor samenwerking lijken bij spam niet aanwezig te zijn. Er is geen bestaande structuur waarbinnen de bij spam betrokken actoren gezamenlijk om de tafel zitten. Geen enkel instituut op de wereld heeft een gezaghebbende rol op het

[80] Frissen, P.H.A. (1996)

gebied van spambestrijding. Overheden, internetproviders, gebruikers en andere actoren werken daardoor vaak langs elkaar heen of komen met oplossingen die regelrecht tegen de belangen van andere actoren ingaan, die daardoor weer (nieuwe) blokkades opwerpen. Van samenwerking is nauwelijks sprake. Het gebrek hieraan is ook te verklaren door het gebrek aan overeenstemming over wat precies het probleem met spam is. De onzekerheid is daardoor te groot om samenwerkingsverbanden aan te gaan.

Het gaat nog verder. Spam is een *wicked problem.* Dat wil zeggen dat er niet alleen gebrek aan overeenstemming is over wat het probleem met (in dit geval) spam precies is; ook over de mogelijke oplossingen zijn de meningen verdeeld. De *inhoudelijke* complexiteit en daarmee onzekerheid over de oplossing van het probleem is groot. Zo zegt bij spam de één dat technische filtering de remedie is, of indien dat niet zou helpen zelfs de creatie van een geheel nieuwe technische opzet van het internet, waarbij spammen veel lastiger zou worden door een nieuw e-mail protocol. De ander meent dat nieuwe wet- en regelgeving de oplossing is. Weer anderen stellen dat er een gebrek aan voorlichting is aan gebruikers van internet. Ook zijn er groeperingen die menen dat spammers een gedrag- of beroepscode af moeten spreken waarin wordt vastgelegd wat wel en niet toegestaan is. En tenslotte zijn er nog voorstanders van het creëren van een digitale postzegel of varianten daarop, waardoor spammers afgeschrikt zouden worden. Al deze varianten kennen hun eigen voor- en nadelen, waar ik in hoofdstuk vier dieper op in zal gaan. Vragen die met de inhoudelijke complexiteit van wicked problems samenhangen zijn: Welke informatie is er beschikbaar over het dilemma dat aan de orde is? Wie levert die informatie aan? Ontbreekt er nog informatie? Of is er wellicht juist een overvloed aan informatie waardoor actoren door de bomen het bos niet meer zien?

Ook op *strategisch* gebied zorgen wicked problems voor uitdagingen. Zo gaat spam over grenzen heen, met als probleem dat er geen wereldwijde spam wet- en regelgeving is. Er is niet één bestaande actor die vanuit een traditioneel hiërarchisch model kan bepalen wat

het spambestrijdingsbeleid zou moeten zijn.[81] Om tot een oplossing van een wicked problem te komen actoren wederzijds van elkaar afhankelijk. Zij worden geforceerd om samen te werken in strategische spelen en netwerken, waarin nieuwe regels en procedures gelden of tot stand moeten komen om tot een oplossing te kunnen komen. Elke actor heeft zijn eigen uitgangspunten, belangen en percepties met betrekking tot een probleem. Het is derhalve moeilijk te voorspellen welke (strategische) keuzes een specifieke actor zal maken.

Er is ook sprake van *institutionele* onzekerheid. Actoren hebben niet alleen eigen belangen, percepties en interesses, ze komen ook nog eens uit verschillende organisaties met verschillende culturen.

Koppenjan en Klijn hebben geprobeerd om een framework te ontwikkelen om met onzekerheid in netwerken om te kunnen gaan. Hun doel is om te kijken of en hoe je onzekerheid in netwerken dusdanig kunt reduceren, dat de betrokken actoren bereid zijn om samen te gaan werken om tot een oplossing van de bestaande problemen te komen. Inzoomen op de inhoudelijke, strategische en institutionele kenmerken van onzekerheid is van belang om een antwoord op deze vraag te krijgen.

Hoe kun je nu voorwaarden scheppen om met onzekerheid om te kunnen gaan? Hoe voorkom je dat er blokkades optreden in het proces en hoe neem je bestaande blokkades weg?

Om dit soort vragen op te lossen moet er gekeken worden naar (de onzekerheid over) inhoud, instituties en strategie. Percepties zijn hier leidend: welk beeld heeft een actor van een bepaalde situatie? Die beelden gebruikt een actor namelijk om betekenis te geven aan

[81] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 1

die situatie en vervolgens om te oordelen over die situatie en over andere betrokken actoren. Op basis van dat oordeel kiest een actor zijn strategie.

4.3.1 Onzekerheid over inhoud

Actoren hebben verschillende percepties van een probleem en bestoken elkaar met hun kennis. Er is vaak echter geen sprake van een dialoog: actoren praten langs elkaar heen, ze luisteren niet naar elkaar. Wildavsky en Tenenbaum spreken in dit kader over een 'Dialogue of the deaf'. Actoren zijn dusdanig overtuigd van het eigen gelijk, dat cognitieve fixatie optreedt, een vorm van groepsdenken waarin nieuwe informatie wordt genegeerd of wordt omgebogen naar eigen inzicht.[82]

Om dit te doorbreken stelt de netwerkbenadering dat er een dialoog moet komen die door de verschillende referentiekaders heen snijdt. Op deze manier kunnen actoren zich bewust worden van de verschillende opvattingen en percepties bij de andere partijen, waarna vervolgens gepoogd kan worden een gemeenschappelijk referentiekader te ontwikkelen. Pas als actoren zich ervan bewust zijn dat niet iedereen hetzelfde referentiekader heeft, is het mogelijk om de echte inhoudelijke vragen te adresseren die om een oplossing vragen.[83]

Om gemeenschappelijke gronden voor samenwerking te bereiken met betrekking tot de inhoud van problemen zijn er samengevat vijf te volgen strategieën:[84]

[82] Wildavsky, A. en E. Tenenbaum (1981)
[83] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 36
[84] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 161

- streef naar gezamenlijke doelen, creëer variëteit door zo lang mogelijk zo veel mogelijk alternatieven open te houden. Hierdoor wordt vroegtijdige fixatie voorkomen.
- doorbreek asymmetrische politieke debatten, door bijvoorbeeld een time-out te nemen of door externe adviseurs in te schakelen.
- maak eerst afspraken over het proces, de inhoud komt later pas. Ook op deze manier kan vroegtijdige fixatie worden voorkomen.
- organiseer selectie op inhoud: houd opties open, stel duidelijke selectiecriteria vast.

Uiteindelijk is het de bedoeling dat deze strategieën leiden tot een verkleining van de afstand tussen de percepties van de verschillende actoren in het proces. Tegelijkertijd leren actoren van elkaar over de inhoud van het probleem. Doordat ze de dialoog met elkaar aangaan als gevolg van deze strategieën, doen ze nieuwe kennis op die hun referentiekader verandert. Zo kan een gemeenschappelijk(er) referentiekader ontstaan, hetgeen samenwerking kan vergemakkelijken.

4.3.2. Onzekerheid over instituties

Onderhandelingen in een netwerksituatie beginnen nooit vanaf nul. Elke actor brengt zijn eigen regels en geschiedenis met zich mee die als uitgangspunt voor de onderhandelingen functioneren. Dit geheel van regels, verhoudingen, waarden en beelden die het gedrag van individuen en organisaties bepalen, noemen we instituties.[85] Deze term wordt hier gebruikt in haar sociologische betekenis en duidt op een complex van gedragsverwachtingen in een bepaald sociaal domein, in dit geval het netwerk. Alle actoren in een netwerk

[85] Derksen, W. (2001)

hebben hun eigen regels, gedragspatronen en taal.[86] Om te kunnen communiceren met de andere betrokken partijen moeten deze grenzen dus eerst geslecht worden.

Het opstellen van (nieuwe) regels voor een strategisch spel kan hiertoe een gezamenlijk referentiekader bieden, zodat de actoren in het spel min of meer weten waar ze aan toe zijn. Het probleem met regels is echter dat je ze ook kunt breken. Daarom is vertrouwen noodzakelijk, want zonder vertrouwen is er geen basis voor samenwerking. Vertrouwen wordt door Koppenjan en Klijn gedefinieerd als het geloof in de goede bedoelingen van anderen.[87] Vertrouwen ontstaat slechts geleidelijk en vereist veel inspanning om te behouden. *'Trust arrives on foot and departs on horseback'*, zo merken Klijn en Koppenjan op.[88] Om een ander te vertrouwen moet je jezelf echter kwetsbaar opstellen, en dat doen actoren in een netwerksituatie liever niet. Het opstellen van regels alleen in een netwerk is dus niet voldoende om onzekerheid te reduceren en samenwerking te bevorderen. Naast het opstellen van regels is het ook van belang om duidelijk te stellen hoe eventuele conflictsituaties worden opgelost en door wie. De aanwezigheid van een arbiter kan actoren ervan weerhouden om het vertrouwen van andere actoren te schaden, daar zij dan de arbiter op hun dak krijgen. Toch zijn de sturingsmogelijkheden van vertrouwen in een netwerk beperkt. Vertrouwen is vooral iets wat door alle maatregelen gezamenlijk moet ontstaan en in stand gehouden moet worden.

Er zijn nog andere manieren om de institutionele setting te veranderen. De eerste strategie is gericht op het wijzigen van de samenstelling van het netwerk: welke actoren laat je wel en niet toe? De tweede strategie is gericht op de uitkomsten die worden nagestreefd: hoe ziet bijvoorbeeld de beloningsstructuur er uit als er een oplossing wordt bereikt? De derde strategie ten slotte richt zich op interacties in het netwerk. Hierbij staat centraal hoe je conflicten kunt smoren en welke procedures daar voor nodig zijn.

[86] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 7
[87] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 84
[88] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 228

4.3.3. Onzekerheid over strategie

Het oplossen van problemen kan worden gezien als een analytische activiteit of als een strategisch spel.[89] Strategieën zijn doel-middel combinaties gebaseerd op percepties die gericht zijn op het beïnvloeden van de inhoud van problemen en oplossingen, de ontwikkeling van het proces en de strategie van andere partijen.[90] Bij probleemoplossing als analytische activiteit is er sprake van een centraal sturende actor die in een proces dat in fasen verloopt probeert te komen tot wetenschappelijk gefundeerde oplossingen. Onzekerheid wordt veroorzaakt door een gebrek aan kennis, en succes wordt behaald als kennisgebrek is gereduceerd door verbetering van de informatievoorziening.

Bij strategische spelen in netwerken daarentegen wordt de realiteit als iets dynamisch gezien, een veranderlijke omgeving waarin geen rechtlijnig proces te ontwaren is, maar waarin alle fasen door elkaar lopen. Het oplossen van problemen is hier een machtsspel waarin spelers wederzijds van elkaar afhankelijk zijn en tot overeenstemming moeten zien te komen. Onzekerheid wordt veroorzaakt door de belangen, posities en voorkeuren van actoren die van elkaar verschillen. Er kunnen voortdurend nieuwe strategieën ingezet worden in eveneens continu wisselende coalities. De onzekerheid is dus groot. En ook ‘Freerider gedrag’ ontstaat snel. Het is immers makkelijker om gewoon alleen maar mee te doen aan een spel, zonder daar verantwoordelijkheid of leiding in te nemen. De kosten van deelname zijn dan veel lager. Actoren zijn daarom geneigd om informatie achter te houden. Hun stelregel is dat er twee regels zijn voor succes:

1. Vertel nooit alles wat je weet.

[89] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 45
[90] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 48

Om onzekerheid over strategie te reduceren moeten de condities voor samenwerking worden aangescherpt. Tevens moet er worden gewerkt aan gezamenlijke beeldvorming over het probleem door middel van facilitatie van het proces, of arbitrage in het proces.

4.4 Management van het netwerk

Om samenwerking van de grond te krijgen moeten de betrokken actoren bij een probleem samen worden gebracht. In een netwerk waarin geen sprake kan zijn van hiërarchische sturing, wat bij het spambestrijdingsprobleem het geval lijkt te zijn, moet er gezocht worden naar een andere manier om het netwerk te 'managen'. In de literatuur wordt in dit kader gesproken over netwerkmanagement. Netwerkmanagement is gericht op het coördineren van strategieën van actoren met verschillende doelen en voorkeuren binnen een netwerk van interorganisationele relaties, met het oog op een bepaald probleem of beleid.[91] Netwerkmanagement is zeker geen eenvoudige opgave door de wederzijdse afhankelijkheid van de betrokken actoren. Een netwerkmanager kan daardoor geen centrale bestuurder of regisseur zijn, maar veeleer een bemiddelaar en stimulator.[92]

Facilitator

Kortom: het spel heeft een *facilitator* nodig. Zo'n facilitator moet aan een aantal voorwaarden voldoen.[93] Hij heeft het vertrouwen nodig van de actoren uit het spel, hij moet neutraal zijn, hij moet over de juiste competenties beschikken en hij moet gezag hebben. Om zijn rol als agendabepaler en -bewaker uit te kunnen voeren heeft hij ook de juiste middelen nodig. Een facilitator is niet verantwoordelijk

[91] Kickert, W.J.M. and J.F.M. Koppenjan (1997) Blz. 43
[92] Klijn, E.H. & J.F.M. Koppenjan (1997) Blz. 150
[93] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 204

voor de inhoud van het proces. Wat hij wel moet doen, is het verkennen van mogelijke kansen. Hij moet actoren, arena's en eventueel spellen aan elkaar koppelen. Hij moet ontmoetingsplaatsen faciliteren, de agenda up-to-date houden, voor zover mogelijk een werkbaar klimaat creëren en hij moet wederzijds begrip bij alle actoren vragen voor de verschillende percepties en belangen die iedereen hanteert.

Tevens moet hij waar mogelijk fixaties voorkomen, hij moet het signaleren als er blokkades opgeworpen dreigen te worden, hij moet zorgen voor voldoende inhoudelijke expertise om de inhoud te bewaken, waar nodig moet hij als scheidsrechter optreden en hij moet ervoor zorgen dat het spel op een eerlijke manier gespeeld kan worden, met gelijke uitgangspunten voor alle actoren.

Kortom: de facilitator of *game manager* moet het proces op gang krijgen, op gang houden en ervoor zorgen dat de samenwerking duurzaam is. De belangrijkste voorwaarde voor succes is dat er bereidheid moet zijn bij de actoren in het spel om een en ander uit handen te geven aan de game manager. Als die bereidheid er niet is, als de onzekerheid hiervoor kennelijk te groot is, dan is de kans van slagen van het managen van een strategisch spel bijzonder klein. En zelfs als die bereidheid er wel is, dan vormen alle regels voor het spel slechts een uitgangspunt. Het spel moet nog steeds gespeeld worden en over de uitkomsten staat nog niets vast. Er zijn immers zoveel actoren met een verscheidenheid aan doelen en strategieën, dat actoren niet van tevoren kunnen weten welke uitkomsten zullen volgen en welke doelen zij in het proces kunnen bereiken. Daar moeten ze tijdens het proces uitkomen.[94]

Ongeacht de gekozen strategie zullen percepties van actoren slechts incrementeel (langzaam, stapje voor stapje) wijzigen door gewijzigde regels of nieuwe kennis en informatie.

[94] Benson, J.K. (1978)

4.5 Concepten en Verbanden

De centrale concepten en de onderlinge verbanden daartussen uit de netwerkbenadering, zijn op basis van het voorgaande als volgt samen te vatten. Door effecten van globalisering is top-down sturing niet altijd meer mogelijk, in een wereld die zich steeds meer kenmerkt door horizontale relaties, zijn actoren in steeds grotere mate wederzijds van elkaar afhankelijk indien zij (complexe) problemen willen oplossen. Maar actoren hebben elk hun eigen percepties van die problemen, en hun eigen geschiedenis, strategieën en doelen. Om tot samenwerking te komen moet er derhalve een gemeenschappelijk referentiekader gesmeed worden. Dit gaat echter niet spontaan, er zal eerst vertrouwen gecreëerd moeten worden tussen de actoren om die samenwerking van de grond te krijgen, dus er is een vorm van netwerkmanagement nodig om dit kader te creëren.

In dit netwerkmanagement staat het reduceren van onzekerheden centraal. Onzekerheden over de inhoud of definitie van het probleem moeten worden aangepakt door een dialoog tussen de actoren te faciliteren. Onzekerheden over instituties kunnen gereduceerd worden door een facilitator aan te stellen die het eventueel aanwezige vertrouwen kan beschermen of anders als aanjager van nieuw vertrouwen kan functioneren. En dit geldt ook voor het reduceren van onzekerheden over strategie, waar een ‘middle man’ zonder direct eigenbelang het vertrouwen kan scheppen dat hard nodig is in een wereld waarin grenzen soms als sneeuw voor de zon gesmolten lijken te zijn en het daardoor onduidelijk is welke actor in welke arena(‘s) opereert, wie daar de macht heeft, of iemand überhaupt nog de macht heeft en wat de gevolgen daarvan zijn voor actoren die hun strategie willen bepalen voor de aanpak van bepaalde problemen.

Kortom: alle mogelijke blokkades en fixaties die er bij actoren kunnen zijn waardoor hun onzekerheid te groot blijft om het vertrouwen te kunnen scheppen dat nodig is voor het creëeren van een gemeenschappelijk referentiekader, moeten worden weggenomen, en een facilitator van het proces of het spel lijkt daarvoor de aangewezen oplossing.

4.6 Conclusie

We hebben gezien dat de staat niet langer altijd de enige gezaghebbende structuur in de maatschappij is. Grensoverschrijdende activiteiten vereisen (wereldwijde) samenwerking in steeds horizontalere netwerken. De veranderende gezagsverhoudingen in deze netwerken leiden tot een nieuw soort, veelal uiterst complexe, problemen (*wicked problems*) die vaak om een nieuw soort oplossingen vragen. Het is hierbij bovenal duidelijk dat eenzijdige actie van actoren niet effectief is. Interactie met andere actoren is noodzakelijk, doordat in netwerken wederzijdse afhankelijkheden zijn ontstaan.

Die interactie kan alleen maar bewerkstelligd worden als actoren elkaar vertrouwen. Maar er is veel onzekerheid onder actoren over de belangen en percepties van anderen. Die onzekerheid moet gereduceerd worden en hiertoe is het van belang om de inhoudelijke, strategische en institutionele kenmerken van onzekerheid te belichten.

Bij de reductie van inhoudelijke onzekerheden is het zaak dat er een dialoog komt tussen actoren die door de verschillende referentiekaders heen snijdt. Op deze manier kunnen actoren zich bewust worden van de verschillende opvattingen en percepties bij de andere partijen, waarna vervolgens gepoogd kan worden een gemeenschappelijk referentiekader te ontwikkelen. Bij de reductie van institutionele onzekerheden zien we dat regels de bindende factor zijn: ze bieden een gezamenlijk referentiekader, zodat de actoren in het spel min of meer weten waar ze aan toe zijn. Strategische onzekerheden draaien om het verbeteren van posities in het spel. Om dit te bewerkstelligen moeten de condities voor samenwerking worden aangescherpt en er moet worden gewerkt aan een gezamenlijke beeldvorming over het probleem door middel van facilitering van het proces of arbitrage in het proces.
Hoe je deze zaken kunt bewerkstelligen was de volgende vraag die op een antwoord wachtte. Het gaat bij de netwerkbenadering om het vermijden van vroegtijdige fixaties, om het bewust maken van de verscheidenheid aan percepties bij de verschillende actoren en

om de voorwaarden te wijzigen of te creëren waardoor het mogelijk wordt om van elkaar te leren en om te zoeken naar gemeenschappelijke gronden voor samenwerking. Hiertoe zijn meerdere strategieën mogelijk:

De inhoudsstrategie is gericht op de verkleining van de afstand tussen de percepties van de verschillende actoren in het proces. Tegelijkertijd leren actoren van elkaar over de inhoud van het probleem. Doordat ze de dialoog met elkaar aangaan als gevolg van deze strategieën, doen ze nieuwe kennis op die hun referentiekader verandert. Zo is het mogelijk dat er een gemeenschappelijk(er) referentiekader ontstaat, hetgeen samenwerking om tot een oplossing van een probleem te komen kan vergemakkelijken. Bij de spelstrategie gaat men ervan uit dat niets zo belangrijk is om in een netwerk gezamenlijk succesvol te zijn in een strategisch spel als een goede set regels. En daarbij hoort een *game manager* die het proces op gang moet krijgen, op gang moet houden en ervoor moet zorgen dat de samenwerking duurzaam is. Het managen van het netwerk draait om het veranderen van de institutionele setting. Strategieën zijn hier gericht op het wijzigen van de samenstelling van het netwerk, op de uitkomsten die worden nagestreefd en op interacties in het netwerk.

Ongeacht de gekozen strategie is het aannemelijk dat verandering in het denken over een probleem slechts met kleine stapjes tegelijk bereikt kan worden.

Hoofdstuk 5
Actoren: belangen en percepties

Inleiding

In dit hoofdstuk komen alle bij spam betrokken actoren en hun belangen en percepties aan bod. Ik zal hier proberen de vraag te beantwoorden hoe het netwerk rondom spam en spambestrijding in elkaar steekt en of en hoe dit gevolgen heeft voor eventuele samenwerking op het gebied van spambestrijding. Dit op basis van het feit dat de 'losse' bestrijdingsmethoden die in hoofdstuk 3 aan de orde zijn gekomen niet voldoende effectief bleken te zijn, en er van uitgaande dat het zelfstandig oplossen van het spamprobleem door de complexiteit van het onderwerp niet mogelijk is.

Door te kijken hoe het netwerk omtrent spambestrijding in elkaar zit, wil ik proberen te achterhalen waarom de actoren zich schijnbaar niet in voldoende mate bewust zijn van het feit dat ze wederzijds van elkaar afhankelijk zijn als ze het spamprobleem willen oplossen. Hebben ze wel een gemeenschappelijk referentiekader, zijn alle onzekerheden wel te reduceren (of al gereduceerd) om voldoende vertrouwen te creëren voor samenwerking?

De empirische basis voor de analyse van de belangen en percepties van de actoren die in dit hoofdstuk aan de orde komen is terug te vinden in paragraaf 1.5 van deze scriptie. Literatuuronderzoek, expertinterviews en praktijkonderzoek hielpen mij in het selecteren van de meest relevante actoren die bij het fenomeen spam betrokken zijn, en in het analyseren van hun percepties, belangen en doelen.

5.1 Actoren: belangen en percepties

In horizontale netwerken is het succes van het beleidsproces afhankelijk van de bereidheid tot samenwerking van de betrokken actoren. De grote vraag bij spambestrijding lijkt dan ook te zijn: waarom komt die samenwerking vooralsnog niet van de grond? Tot dusverre zijn er weinig initiatieven geweest om bijvoorbeeld wetgeving, voorlichting en technische filtering beter op elkaar aan te laten sluiten. Zowel in Nederland als wereldwijd is er slechts sprake van losse eilandjes die allemaal zelf proberen met een oplossing te komen. Om het gebrek aan samenwerking te verklaren moet in kaart worden gebracht wie de betrokken actoren zijn en wat hun belangen en percepties zijn. Is er sowieso wel sprake van interactie of zitten alle actoren in verschillende netwerken die niet of niet voldoende aan elkaar verbonden zijn? En waar worden de beslissingen over spambestrijding genomen? In welke arena's? En zijn die aan elkaar gekoppeld? In hoeverre zijn de actoren van elkaar afhankelijk om hun doelen te bereiken?

Hier probeer ik dus de theoretische bevindingen uit hoofdstuk 4 te vertalen naar de praktijk. Is de onzekerheid waar ik het daar over had inderdaad te reduceren en biedt dit voldoende perspectief voor een oplossing van het spamprobleem? Kortom, zoals in de inleiding van dit hoofdstuk al gesteld werd: wordt er bij spambestrijding voldaan aan de voorwaarden die de netwerkbenadering stelt aan een succesvolle manier van het benaderen van een beleidsproces of is de praktijk weerbarstiger?

De actoren die aan bod komen in dit hoofdstuk zijn consumenten, de zakelijke markt, direct marketeers, internet service providers, de media en overheden.

5.1.2 Consumenten

De consument is een van de belangrijkste betrokken actoren bij het spamprobleem. Honderden miljoenen consumenten wereldwijd ontvangen dagelijks spam. De Transatlantic Consumer Dialogue (TACD) is een forum bestaande uit 65 Amerikaanse en Europese consumentenorganisaties dat in 2003 onderzoek gedaan heeft naar de opvattingen van consumenten over spam.[95] Een aantal van de belangrijkste bevindingen van dat onderzoek:

- 96% van de ondervraagde consumenten gaf aan spam te haten of er geïrriteerd door te raken.
- 83% gelooft dat vrijwel alle spam e-mails frauduleus of misleidend zijn.
- 65% is van mening dat spam de consument of de werkgever geld kost.
- 62% gebruikt een spamfilter, maar slechts 17% vindt dat filter effectief genoeg**.**

De opvattingen over het spamprobleem van consumenten zijn hiermee helder. De positie die zij innemen is dat ook, zo blijkt uit uit nog twee resultaten van het onderzoek:

- 84% vindt dat alle spam verboden moet worden.
- 81% vindt dat commerciële e-mails alleen met goedkeuring van de ontvanger verstuurd mogen worden (opt-in).

Het onderzoek van de TACD staat niet op zichzelf. In hoofdstuk 1 gaf ik al aan dat uit onderzoek van Interview NSS uit 2002 blijkt dat maar liefst 85,2% van de Nederlanders -uit een steekproef met 15.000 respondenten- ongevraagde e-mail als irritant beschouwt .[96] Er

[95] TACD (2004) Consumer Attitudes Regarding Unsolicited Commercial Email (spam)
[96] Interview-NSS (2002)

worden wereldwijd voortdurend dit soort onderzoeken gedaan die allemaal ongeveer dezelfde resultaten hebben. Consumenten willen dus van spam af. Als individu kunnen ze niet veel meer doen dan een spamfilter aanbrengen en goed uitkijken waar ze hun e-mailadres allemaal publiceren. Als collectief, bijvoorbeeld verenigd in een consumentenbond, kunnen ze proberen om druk uit te oefenen op overheden om met betere wet- en regelgeving of andere oplossingen te komen.

Een paradoxale keerzijde aan dit verhaal is te vinden in de voorlopige bevindingen (maart 2005) uit een onderzoek van de Radicati Groep in samenwerking met Mirapoint. Hieruit blijkt dat ruim 30 procent van de internetters zegt wel eens op linkjes in spamberichten te klikken. En een op de tien respondenten zegt wel eens een product gekocht te hebben dat via spam werd aangeprezen. Hoe spam in dit onderzoek gedefinieerd is en hoe groot de groep respondenten is, is echter onduidelijk. Meer informatie over het onderzoek is nog niet vrijgegeven.[97]

5.1.3 Zakelijke markt

De zakelijke markt ofwel het bedrijfsleven is een geval apart bij het spambestrijdingsprobleem. Het onderscheid tussen een zakelijke en privé-ontvanger van e-mail is nauwelijks te maken. Veel mensen gebruiken hun e-mailaccount voor zowel zakelijke als privé aangelegenheden. Bij het tot stand komen van nieuwe wet- en regelgeving is er dan ook vaak onduidelijkheid over het onderscheid.

[97] De voorlopige resultaten werden bekend gemaakt door middel van een openbare brief, die te lezen is op www.radicati.com/email_survey2005.shtml.

'Legal persons are not protected by the general regime of the Data Protection Directive. According to article 13(5), subscribers other than natural persons are exempt from the protection of paragraphs 1 and 3 of Article 13.'[98]

Maar ook zakelijke gebruikers van het internet hebben last van spam. In hoofdstuk 1 gaf ik ook hier voorbeelden van, zoals het onderzoek van Nucleus Research dat stelde dat Amerikaanse bedrijven 874 dollar per werknemer per jaar kwijt zijn als gevolg van spam door verloren arbeidsproductiviteit. En de berekening van Ferris Research dat bedrijven en providers wereldwijd op jaarbasis bijna twaalf miljard dollar kwijt zijn aan het verwerken en tegengaan van spamberichten.

Voor het bedrijfsleven is het niet alleen vanuit irritatie over spam dus van groot belang dat spam bestreden wordt, maar vooral ook uit economisch belang. De lobby van direct marketeers is echter soms zo groot, dat ze het kunnen doen voorkomen alsof het bedrijfsleven juist baat zou hebben bij ongewenste e-mail. De situatie wordt dan omgedraaid, het gaat dan niet over het ontvangen van ongewenste e-mail, maar over het verzenden. Bedrijven zouden dit volgens direct marketeers moeten willen, omdat zij zo op een goedkope manier (potentiële) klanten kunnen benaderen. De invloed van direct marketeers reikt ver:

'Tijdens de bespreking van de anti-spamwet in de Tweede Kamer in november 2003, had de PvdA voorgesteld ook spam te verbieden die gericht is op het bedrijfsleven. Daar ging het CDA toen dwars voorliggen. Deze partij volgde de opvatting van werkgeversorganisatie VNO/NCW. Die verklaarde zonder overleg met haar achterban dat zo'n verbod niet nodig was. Na kritiek uit eigen gelederen herzag de organisatie haar standpunt. Vervolgens draaide ook het CDA bij.'[99]

[98] IviR (2004) Blz. 36
[99] Laan, Marc (2004)

De meeste gewone bedrijven zijn zich echter bewust van de schade die het versturen van spam aanbrengt aan het imago van het bedrijf en kijken dus vooral naar het ontvangen van spam als het gaat om hun positiebepaling bij spambestrijding. En dan zijn zij net als consumenten dus eensgezind van mening dat spam bestreden moet worden. De nuance is bij het bedrijfsleven vooral te vinden in de discussie over opt-in en opt-out. Om toch de optie open te houden om zelf ongevraagde e-mails te versturen pleiten sommige bedrijven voor het opt-out regime.

5.1.4 Direct marketeers

Er zijn twee categorieën direct marketeers. De ene categorie houdt zich bezig met het op een legitieme manier versturen van e-mails, de andere categorie besteedt juist geen enkele aandacht aan wet- en regelgeving. Die laatste groep is de oorzaak van de grote hoeveelheden spam met vervalste afzenderadressen en vreemde leestekens om filters te ontlopen. Het gaat dus kort gezegd over het verschil tussen legitieme direct e-mail en spam.

Legitieme direct e-mail

Bedrijven of personen die zich met legitieme direct e-mail bezig houden proberen aan wet- en regelgeving te voldoen. Soms zijn zij verenigd in een branche-organisatie die niet alleen de wettelijke regels als uitgangspunt heeft, maar die ook zelfregulering probeert toe te passen om aan de wensen en eisen van de ontvangers van e-mailberichten te voldoen. Dit soort direct marketeers wil graag gebruik maken van e-mail om hun potentiële klanten te benaderen, omdat de kosten van het versturen van grote hoeveelheden e-mails heel erg laag zijn. Direct marketeers zijn in de regel voorstander van het opt-out systeem, zodat hun mogelijke doelgroep zo groot mogelijk

blijft. Dit gaat in tegen de wens van de consument en de (Europese) wet die inmiddels uitgaat van het opt-in principe. De belangen van direct marketeers botsen dus met die van andere bij spambestrijding betrokken actoren.

Spam

De andere categorie direct marketeers zijn de echte spammers. Zij zijn zo goed als ongevoelig voor wet- en regelgeving, voor de wensen van consument of bedrijfsleven en voor allerlei andere maatregelen die welke actor dan ook onderneemt. Hun enige belang is om hun boodschap op zoveel mogelijk adressen af te leveren zodat de potentiële klantenkring zo groot mogelijk is. Zij zijn in tegenstelling tot gewone bedrijven of legitieme direct marketeers niet gevoelig voor imago-schade. De bedrijfsnaam (indien daar al sprake van is) is toch onbekend, het gaat puur om het verkopen van het aangeboden product. En bij een volgende spamrun is de afzender toch weer iemand anders (althans, zo doen ze het lijken).

Bij dit soort spammers is dus geen sprake van een legitimiteitsvraagstuk of afhankelijkheid van andere actoren. Los van alle andere actoren kunnen zijn hun eigen beleid uitstippelen. Het enige waar zij last van hebben zijn de maatregelen die de andere actoren bedenken om spam te weren. Zelf zijn ze zich vaak niet eens bewust van het probleem, of beweren dat in ieder geval. In een interview met het blad Management Team[100] verbaast spammer Patrick Platenkamp zich over het grote aantal spamhaters: “Ik vind het overdreven. Als je niet blij bent met een reclamefolder in je brievenbus, gooi je die toch ook gewoon weg.”

[100] Bakkeren, Hanno (2004)

5.1.5 Internet Service Providers

Internet Service Providers (ISP's) hebben net als het bedrijfsleven belang bij het weren van zoveel mogelijk spam. De kosten voor ISP's om spam te bestrijden zijn gigantisch. Zo is de Nederlandse internet provider XS4ALL jaarlijks 368.000 EUR kwijt aan extra servers en personeel om spam te weren.[101]

Economische motieven spelen bij ISP's dan ook de grootste rol. Een opt-in regime vinden zij het meest wenselijk, daar dit in theorie het aantal spam e-mails het meeste zou beperken. Daar wet- en regelgeving niet voldoen zijn ISP's gedwongen om zelf maatregelen te nemen. Zoals bijvoorbeeld het aanbrengen van technische spamfilters, omdat ze bang zijn dat hun klanten anders weg gaan. Maar ze lokken ook rechtszaken uit tegen spammers om zowel de druk op overheden te houden om met betere wet- en regelgeving te komen, als om spammers uit te schakelen die het (inter)netwerk zwaar belasten.

5.1.6 De media

De media hebben een aparte rol bij spambestrijding. Zij voeren geen actief anti-spam beleid, maar brengen in kaart wat de ontwikkelingen op dit gebied zijn. Door dit te doen lichten zij al dan niet impliciet het publiek voor over mogelijke anti-spam maatregelen. Berichtgeving over spam kan er toe leiden dat het publieke debat verhevigd wordt, wat weer aanleiding kan zijn voor politici om spam op de politieke agenda te plaatsen. De media hebben geen baat bij een opt-in of opt-out regime. Zij hebben baat bij welke mogelijke vorm van berichtgeving over spam dan ook.

[101] Reijnders, Maarten (2002)

5.1.7 Overheden

Overheden zijn een belangrijke actor bij spambestrijding. Politici moeten het probleem op de politieke agenda zien te krijgen en bestuurders zijn vervolgens verantwoordelijk voor het opstellen van wet- en regelgeving die spam al dan niet aan banden legt.

Het probleem bij het woord overheid is dat zich direct de vraag aandient: over welke overheid heb je het? Bij spambestrijding zijn de overheden die betrokken zijn in de regel de nationale overheden, maar niet atijd. In de Verenigde Staten waren het juist gedurende lange tijd de federale staten die wet- en regelgeving op het gebied van spambestrijding regelden. Pas dit jaar trad de nationale CAN-SPAM act in werking. In Europa is een soortgelijke beweging zichtbaar. Eerst hebben sommige nationale staten zelf geprobeerd met anti-spam maatregelen te komen, later is dit in supranationale Europese wet- en regelgeving vastgelegd in de vorm van richtlijnen, die de aangesloten lidstaten vervolgens moesten implementeren in hun nationale wetgeving.

Spambestrijding binnen overheden vindt dus vooralsnog op drie niveaus plaats:

- (in federale staten) op federaal niveau
- op nationaal niveau
- op supranationaal niveau

Maar voor de beweegredenen van overheden om spam te bestrijden blijkt het niveau niet uit te maken. Het probleem is bij alle lagen hetzelfde: spam zorgt voor economische en sociale schade bij zowel consumenten, bedrijfsleven als bij de overheid zelf, waar ook veel spam wordt ontvangen en gefilterd moet worden. Motieven voor overheden om spam te bestrijden variëren. Argumenten kunnen zijn: de bescherming van privacy (EU), ‘huisvredebreuk’ en het tegengaan van overlast (VS), het corrigeren van marktfalen (zelfregulering

blijkt niet mogelijk), het beschermen van een publiek belang (indien politici e-mail tot publiek belang uitroepen, wat soms gebeurt met een beroep op de ontwikkeling van internet tot nutsvoorziening). Argumenten voor overheden om zich juist niet met spambestrijding te bemoeien kunnen zijn dat de markt het probleem zelf moet oplossen (Brinkhorst), of dat het probleem te complex is (spam is grensoverschrijdend, het is ondoenlijk om alle actoren te kennen, en wet- en regelgeving moet grensoverschrijdend zijn maar er is geen supranationale instantie die hiertoe bevoegd is).

'De overheid' bevindt zich als actor dan ook in een uitzonderlijke positie. Zij moet namelijk een normatieve (politieke) afweging maken of ze überhaupt wel een rol *moet* spelen bij spambestrijding. Deze discussie wordt vaak ontlopen door in te gaan op de vraag of ze een rol *kan* spelen. Het antwoord daarop is in de praktijk dus 'ja', anders zou er in het geheel geen sprake van overheidsvoorlichting en/of wet- en regelgeving op het gebied van spambestrijding zijn. De vragen welke overheid dit dan zou moeten doen en welke rol voor deze overheid weggelegd is, staan dan nog steeds open.

5. 2 Het spel

Nu de actoren, hun belangen en percepties benoemd zijn, is de volgende vraag: in welke arena's vindt besluitvorming over spambestrijding nu plaats en waar treedt (eventueel) stagnatie op?

Besluitvorming over spambestrijdingsmaatregelen vindt veelal in eigen kring plaats. Daarmee bedoel ik dat de actoren zelf dat regelen wat binnen hun eigen straatje past. Desondanks is overal het besef aanwezig dat actoren het spamprobleem op eigen houtje niet kunnen oplossen. Zo zagen we consumenten niet alleen met spamfilters werken, maar ook proberen druk uit te oefenen op overheden om met betere wet- en regelgeving of andere oplossingen te komen. Ook bedrijven pleiten daar bij overheden voor. Direct marketeers hebben contacten met in ieder geval het bedrijfsleven om te weten wat hun doelgroep (want dat is het bedrijfsleven) wil. En met

overheden om de totstandkoming van wet- en regelgeving te beïnvloeden. ISP's op hun beurt brengen niet alleen technische filters aan, maar lokken ook rechtszaken uit tegen spammers om steeds betere wet- en regelgeving te forceren. En de media doen niet zozeer direct mee aan besluitvorming over spambestrijding, maar ze spelen wel een rol in de opinievorming. Overheden ten slotte hebben als enige actor contact met alle andere actoren. Meestal niet zozeer uit eigen initiatief, maar omdat die andere actoren bij de overheid aankloppen omdat ze er zelf niet uit komen.

Spambestrijding lijkt te stagneren bij twee actoren: spammers die zich van niets of niemand iets lijken aan te trekken en overheden die niet op een effectieve wijze kunnen of willen ingrijpen. De utopie dat internet zichzelf reguleert blijkt vooralsnog niet meer dan dat te zijn: een ideale situatie die in de praktijk niet bestaat. Spamfilters en voorlichting aan internetgebruikers zouden gezien kunnen worden als een poging tot die zelfregulering, maar die volstaan niet. En dan gaan spamfilters nota bene al over grenzen heen. Meer kunnen ISP's en internetgebruikers niet doen. Wet- en regelgeving gaan echter nog steeds nauwelijks over grenzen heen, daar is dus nog een wereld te winnen. Besluitvorming op een supranationaal niveau dat geen aandacht meer schenkt aan territoriale grenzen is immers noodzakelijk, maar ontbreekt.

Het probleem met het spel van spambestrijding is dat er verschillende arena's zijn die als losse eilandjes functioneren. Alle actoren vinden het wiel voortdurend opnieuw uit. Elke internet provider heeft zijn eigen spamfilter, elke overheid heeft zijn eigen wet- en regelgeving, et cetera. Slechts sporadisch werken overheden of andere actoren onderling samen, maar samenwerking met andere actoren, of serieuze grensoverschrijdende samenwerking zijn nauwelijks aan de orde. [102] Een extra probleem hierbij is dat de belangrijkste arena waar het spel gespeeld zou moeten worden, het internationale podium, momenteel de structuur en instituties

[102] In het begin van het volgende hoofdstuk is een grafische weergave te vinden van de diverse arena's (6.1)

ontbeert die beleidsbeslissingen kunnen formaliseren en legaliseren. Het spel ontbeert het hoogste niveau waarop het gespeeld zou moeten worden.

5.3 Netwerk en Analyse

Wederzijdse afhankelijkheden

De betrokken actoren zijn zich er van bewust dat ze door het grensoverschrijdende karakter van spam in een netwerk zitten waarbinnen ze elk slechts geringe sturingsmogelijkheden hebben. Om tot een effectieve(re) oplossing van het spamprobleem te komen zouden de betrokken actoren wederzijds van elkaar afhankelijk moeten zijn. Maar het besef dat ze dat zijn is niet voldoende aanwezig. Als overheden stoppen met wet- en regelgeving kunnen ISP's, consumenten en bedrijfsleven gewoon doorgaan met technische filters. En als ISP's stoppen met filtering belet dit overheden niet om door te gaan met het opstellen van wet- en regelgeving en de (uitbreiding van) handhaving daarvan. Maar met die losse maatregelen alleen wordt spam niet teruggedrongen, het is juist de combinatie van maatregelen die spambestrijding zo effectief mogelijk maakt. Met alle actoren om de tafel gaan zitten om tot de optimale oplossing te komen lijkt dus de juiste strategie, maar die wordt nauwelijks gevolgd.

Gemeenschappelijk referentiekader

Dat er desondanks soms toch ad hoc interactie tussen de betrokken actoren bestaat komt doordat vrijwel alle betrokkenen toch ergens de notie hebben dat de maatregelen op de een of andere manier aanvullend zijn. Consumenten, ISP's en bedrijfsleven zoeken naar houvast in hun strijd tegen spam en vinden in een overheid die aan hun zijde mee strijdt tegen de vijand een bondgenoot en een

hopelijke aanvulling die er toch iets toe doet (elke spammer die wordt afgeschrikt door wetgeving is er één minder). En overheden hebben te maken met een legitimiteitsvraagstuk. Als zij niets doen verliezen ze het vertrouwen van de consument en het bedrijfsleven, die zich vervolgens kunnen wreken in een andere hoedanigheid. Namelijk die van kiezer. Maar retoriek wint het dan soms van daadwerkelijke actie.

Zo vond de Finse Eurocommissaris Erki Liikanen in februari 2004 dat een mondiale aanpak noodzakelijk is om spam echt effectief aan te kunnen pakken. Hij doet vijf aanbevelingen:

1) Effectieve wetgeving tegen spam in alle landen
2) Samenwerking tussen opsporingsinstanties voor vervolging
3) Coördinatie in zelfregulering door de internetbranche
4) Stimulering van technische oplossingen
5) Beter bewust maken van internetters zelf

Maar laat vervolgens weten dat de organisatie van industrielanden OECD het voortouw moet nemen in de uitvoering hiervan. De Europese Commissie schuift het probleem zo weer naar een andere actor zonder zelf direct een concrete bijdrage te willen leveren.[103]

En daarmee blijft het feit dat de samenwerking niet structureel is, een probleem op drie niveaus. Ten eerste is de samenwerking die er is, gefragmenteerd. De consumentenbond die lobbiet bij minister Donner (Justitie). VNO-NCW namens het bedrijfsleven bij minister Brinkhorst (Economische Zaken). De brancheorganisatie NLIP bij de Europese Unie. Wat nodig zou zijn is dat alle

[103] Planet Internet (2004)

consumentenbonden, het bedrijfsleven en internetproviders wereldwijd zich verenigen in een uitspraak over spam vanuit hun gezichtspunt. Ten tweede zitten die verenigde consumentenbonden, bedrijfsleven en internetproviders niet met elkaar om de tafel. En ten derde worden er (daardoor) nauwelijks grensoverschrijdende maatregelen genomen.

Interactie, arena's en wederzijdse afhankelijkheid

Ergens is er dus wel het besef dat samenwerking noodzakelijk is om spam optimaal te bestrijden, maar de interactie die er is tussen de betrokken actoren bestaat of niet, of op het verkeerde niveau. Beslissingen worden hierdoor op te lage niveaus genomen, zoals op het gebied van wet- en regelgeving in federale staten in de Verenigde Staten of door de Europese Commissie. Ook ISP's, bedrijfsleven en consumentenbonden zijn onvoldoende aan elkaar gekoppeld. Spambestrijdingsmaatregelen zijn hierdoor niet grensoverschrijdend, hetgeen wel noodzakelijk is om spam optimaal te bestrijden. Er is wel sprake van wederzijdse afhankelijkheid, maar die wordt nog onvoldoende door de betrokken actoren herkend.

Top-down sturing

Top-down sturing van de overheid waar de meeste actoren om vragen (wet- en regelgeving als vangnet van spambestrijdingsmaatregelen) is in theorie wel mogelijk, maar in de praktijk niet omdat er geen grensoverschrijdende overheidsinstantie is die de bevoegdheid heeft om spambestrijdingsmaatregelen te nemen die wereldwijd gelden.

Onzekerheid over strategie

Daarnaast is het internet nog steeds relatief jong. Het spamprobleem is zelfs nog jonger, de echt grote hoeveelheden spam worden pas sinds ongeveer 2000 verstuurd, hoewel de eerste spam e-mail al uit 1978 dateert. Het lijkt er daarom ook op dat de actoren die door spam getroffen worden nog bezig zijn om hun posities te kiezen en het speelveld te leren kennen. Er is niet zozeer onwil om samen te werken met andere actoren bij de meeste actoren, maar vaak zijn de andere actoren gewoon nog onbekend. Het gebrek aan historische relaties tussen de verschillende actoren op het gebied van spambestrijding bevordert samenwerking niet.[104]

Als het speelveld de spelers niet geheel duidelijk is, omdat zoals eerder gesteld het hoogste spelniveau de structuur en instituties ontbeert die nodig zijn, dan wordt de te kiezen strategie voor de spelers ook heel lastig. De actoren die bij het spamprobleem betrokken zijn hebben al moeite genoeg om voor hun eigen klanten (of burgers in het geval van overheden) een strategie te verzinnen die direct effect heeft, laat staan dat ze ook nog eens moeten samenwerken met andere actoren, eventueel zelfs in andere landen. Hierdoor ontstaan er zoveel onzekere factoren, dat actoren niet snel geneigd zullen zijn om risico's te nemen. En alles wat nieuw is, is een potentieel risico. De neiging om de status quo te handhaven als er teveel onzekerheden zijn is groot.

Desondanks is grensoverschrijdende samenwerking tussen consumentenbonden, bedrijfsleven en ISP's langzaam aan het toenemen. Bij overheden is dat een ander verhaal. Grensoverschrijdende samenwerking wordt door hen vaak gezien als een verlies van soevereiniteit. Het overdragen van bevoegdheden naar supranationale niveaus gaat in de regel niet zonder slag of stoot, dat is dagelijks zichtbaar in de discussie binnen de Europese Unie over het overdragen van bevoegdheden van nationale lidstaten naar het EU-niveau. Toch zie je ook daar dat het aantal overgedragen bevoegdheden alleen maar toeneemt naarmate de tijd verstrijkt.

[104] Rogers, D.L. & Whetten, D.A. (1982)

Globalisering, internationalisering en de daarmee samenhangende deterritorisalisering lijken niet af te stoppen te zijn. Het is dus wellicht niet zozeer de vraag *of* er grensoverschrijdende samenwerking komt tussen overheden, of beter gezegd nationale staten, maar vooral *wanneer* en *hoe*.

Onzekerheid over instituties

Maar de onzekerheid die nationale staten hier over hebben is nu in ieder geval nog te groot om ineens doortastend actie te ondernemen. Dit soort grensoverschrijdende samenwerking is nog te weinig geïnstitutionaliseerd. Zo weinig zelfs, dat er –zoals gezegd- niet eens een instituut bestaat dat op dit niveau bevoegdheid heeft. De meest verregaande internationale vormen van samenwerking zijn zichtbaar in organisaties als de Organisation for Economic Co-operation and Development (OECD) en de Verenigde Naties, maar die hebben beide hun beperkingen.

De OECD omhelst slechts 30 lidstaten die zich inzetten voor met name economische ontwikkeling en democratie. Er zijn contacten met nog eens 70 staten, maar veel meer dan onderzoeksmateriaal aanleveren en adviseren over in te zetten instrumenten bij bepaalde problemen kan de OECD niet.[105]

De Verenigde Naties (VN) hebben een breder mandaat. In het Handvest van de Verenigde Naties is het ontwikkelen van internationale wetgeving als taak voor de VN vastgelegd. Er zijn inmiddels al meer dan 500 juridisch bindende standaarden, verdragen en conventies gerealiseerd binnen de VN. [106] 23 daarvan vallen onder de eerder genoemde World Intellectual Property Organization (zie hoofdstuk

[105] OECD (2004) About OECD
[106] UN (2004)

1), een internationale organisatie die het gebruik en de bescherming van intellectueel eigendomsrecht promoot.[107] Met 181 aangesloten lidstaten zou de WIPO een grote rol kunnen spelen op het gebied van spambestrijding, maar de doelstellingen van de WIPO liggen te ver af van het onderwerp spambestrijding. Nu liggen die doelstellingen wel onder vuur, zo bleek op een internationale workshop van de TACD met als onderwerp ‘'The Future Of WIPO – ‘Property has duties as well as rights' - A new mission for WIPO”.[108] Maar voorlopig richt de kritiek zich daarbij vooral op de juiste afweging van private en publieke belangen. Van een wezenlijke taakuitbreiding waardoor spambestrijding prominent op de agenda van de WIPO zou komen is vooralsnog geen sprake.

Los van onzekerheden over instituties van overheden, zijn ook de andere actoren onzeker over elkaar. En dan gaat het niet eens direct over eventueel wantrouwen van internet providers jegens spammers, of van consumenten jegens internet providers, maar alleen al tussen die actoren onderling kunnen er onzekerheden zijn. Elke provider hanteert een andere bedrijfsfilosofie en heeft zijn eigen methoden om spam te bestrijden. Consumenten kunnen bijzonder goed op de hoogte zijn van de werking van spam en alle maatregelen nemen om spam te voorkomen, maar ze kunnen ook onwetend zijn van de werking en door dit gebrek aan kennis de toename van spam juist bevorderen. Of erger: al dan niet bewust kunnen ze ervoor zorgen dat de consumenten die juist zo hard bezig zijn om spam te voorkomen, toch spam krijgen. Bijvoorbeeld indien ze een virus verspreiden waardoor spam naar het adres van die andere consument gaat.

Er is dus veel ruis op de lijn, zowel binnen als tussen (groepen van) actoren, waardoor de onzekerheden groot zijn.

[107] WIPO (2004)
[108] TACD (2004) The future of WIPO

Onzekerheid over inhoud

De onzekerheid is ook nog aanwezig op het gebied van de inhoud. Wat het probleem met spam precies is wordt door de verschillende actoren anders ervaren. Consumenten vinden spam irritant en een inbreuk op hun privacy en willen opt-in wetgeving. Bedrijven zijn niet eenduidig in hun opvattingen over spam. Een deel heeft dezelfde opvatting als consumenten en wil derhalve ook een opt-in regeling, een ander deel wil de optie openhouden om zelf e-mail als direct marketing instrument te kunnen gebruiken. En op die opvatting sluiten direct marketeers dan ook aan. Zij willen ook opt-out regelgeving, maar liefst nog helemaal geen regelgeving: zelfregulering is volgens hen de oplossing. ISP's zien spam als een economisch en technisch probleem en overheden ten slotte hebben uiteenlopende opvattingen. Spam wordt door hen gedefinieerd als economisch, juridisch, sociaal of technisch probleem, waarbij de vraag door wie spam bestreden moet worden voortdurend wisselende antwoorden krijgt, afhankelijk van de politieke constellatie van het betreffende overheidsorgaan. En indien het antwoord luidt dat overheden moeten helpen door wet- en regelgeving op te stellen, dan dienen de volgende onzekerheden zich alweer aan, namelijk onzekerheid over de definitie van spam (zie 2.3) en de daardoor complexe wet- en regelgeving door onder andere de voortdurende discussie over opt-in of opt-out oplossingen (zie 4.5).

'Sense of urgency'

Ten slotte is er ook te weinig druk van buitenaf om meer en betere samenwerking te forceren. Op de politieke agenda staan wereldwijd veel dringendere issues, zoals terrorismebestrijding en de vraag hoe de economische recessie het beste kan worden tegengegaan. Het publieke debat over spambestrijding ligt mede daardoor ook enigzins stil sinds pakweg begin 2004, virusbestrijding heeft nu wereldwijd de aandacht. Dat de twee onderwerpen gerelateerd zijn komt lang niet altijd naar voren. Het bedrijfsleven heeft zich in het hele spamdebat tot nu toe sowieso enigzins afzijdig gehouden, terwijl de economische kosten van spam in allerlei onderzoeken keer op keer hoog uit blijken te vallen. Maar de meeste individuele bedrijven hebben zelf de kosten nooit in kaart gebracht, waardoor de

‘sense of urgency’ veelal ontbreekt. Het management bij veel bedrijven bestaat dan ook vaak nog uit een generatie die niet met internet is opgegroeid. Men weet niet hoe het internet werkt, het verschijnsel spam is bij het management vaak onbekend, maar op de werkvloer worden werknemers er mee doodgegooid. Bedrijven die de berekeningen wel gemaakt hebben (zoals ISP’s) voelen de sense of urgency wel, maar dat is een kleine groep.

5.4 Conclusies

Samenvattend komt de samenwerking bij spambestrijding nog niet voldoende van de grond door een aantal factoren. Ten eerste zijn de onzekerheden over inhoud, instituties en strategie nog te groot. Ten tweede er is wel een gemeenschappelijk referentiekader (spam moet bestreden worden), maar binnen dat kader lopen de meningen nog te veel uiteen. Ten derde zijn er nauwelijks blokkades voor interactie en zelfs top-down sturing zou mogelijk zijn, maar er ontbreekt een instituut waarbinnen die interactie en sturing plaats kunnen vinden. Ten vierde is er geen sprake van bewuste of opzettelijke geslotenheid van actoren, maar de meeste actoren handelen nog niet echt open. Hetgeen weer te maken heeft met het vijfde punt: het onvoldoende aanwezige besef dat de actoren bij spambestrijding wederzijds van elkaar afhankelijk zijn.

In een netwerksituatie worden de grenzen van het spel bepaald door de onderlinge verhoudingen. Die zijn in principe goed, er is een gemeenschappelijke vijand (de spammer) alleen is de coalitie van de ‘good guys’ nog niet helder gedefinieerd door de actoren zelf. Om het spamprobleem toch op de agenda te krijgen en te houden worden er in de praktijk deelcoalities gesmeed om toch alvast iets te doen. Het rapport van de TACD en de werkconferentie van de OECD zijn hier voorbeelden van. Een probleem hierbij blijft dat de betrokken actoren niet in een hiërarchische relatie tot elkaar staan. Niemand kan maatregelen bij een ander afdwingen. Daarom blijft het onvoldoende besef van de wederzijdse afhankelijkheid toch een groot struikelblok.

Ook is er sprake van een botsing tussen de opvatting of spam nu door de markt bestreden moet worden (privaat), door de overheid (publiek) of door overheid en markt samen (publiek-privaat). Vrijwel alle actoren opteren voor die laatste optie, maar overheden zelf wijzen nog vaak naar een marktoplossing, hoewel daar verandering in lijkt te komen. Dit is bijvoorbeeld te zien door de uitspraken van minister Brinkhorst van begin en eind 2004 te vergelijken. Waar hij aanvankelijk nog stelde dat de markt het spamprobleem zelf maar moest oplossen, is hij een half jaar later bezig met een door de overheid geïnitieerde voorlichtingscampagne.

Indien er wordt gekozen voor (onder andere) een juridische oplossing, werkt samenwerking vaak niet door de onzekerheid over de definitie van spam en de daardoor complexe wet- en regelgeving door onder andere de voortdurende discussie over opt-in of opt-out oplossingen. Het gaat dan niet zozeer over onwil bij overheden, maar het inzicht ontbreekt vaak gewoon. De verschillen in de bestuurlijke en politieke systemen tussen nationale staten vormen hierbij een extra belemmering. En zelfs relatief onbelangrijk lijkende factoren als afstand en taal- en cultuurverschil kunnen obstakels vormen. Zo hebben al deze factoren tezamen tot gevolg dat er van een grensoverschrijdende aanpak van de spamproblematiek geen sprake is. En omdat er geen grensoverschrijdende aanpak is, doen alle actoren op lager niveau dan ten minste maar datgene wat ze zelf kunnen doen, onder het motto: ‘het is dweilen met de kraan open, maar je moet toch iets.’

Tot dusverre is in kaart gebracht wat spam precies is, hoe het werkt, wat de problemen met de definitie zijn en dat spam niet alleen problemen veroorzaakt maar zelf ook een gevolg is van deterritorialisering. Aansluitend werd er gekeken welke bestrijdingsmogelijkheden er zijn en of samenwerking hierbij nodig is. Het antwoord hierop is ja. Daarna was de vervolgvraag welke actoren er bij het spambestrijdingsbeleid betrokken zijn en of en wáárom samenwerking niet van de grond komt. Nu ook die vraag beantwoord is, rest slechts de vraag: hoe dan wel? En welke rol kan de overheid (en welke overheid) hier dan bij spelen? Die laatste vragen worden behandeld in het volgende hoofdstuk.

Hoofdstuk 6
Bouwstenen voor een oplossing

6.1 Naar een gemeenschappelijk referentiekader

De combinatie van het in kaart brengen welke actoren er allemaal betrokken zijn bij spambestrijding, welke spambestrijdingsmaatregelen er mogelijk zijn en het verkennen van de posities en belangen van de actoren leidt in dit hoofdstuk tot een poging om bouwstenen aan te dragen voor een oplossing van de spamproblematiek. Als de huidige maatregelen niet voldoende effectief zijn en de noodzakelijke samenwerking niet tot stand komt, hoe moet het dan wel?

Het uitgangspunt van dit hoofdstuk is dat spambestrijding pas optimaal effectief is als er door alle (meest relevante) betrokken actoren –ISP's, consumenten(organisaties), overheden, direct marketeers en bedrijfsleven- wordt samengewerkt. De aanpak moet bestaan uit een combinatie van mogelijke spambestrijdingsmaatregelen: wet- en regelgeving (en daadwerkelijke handhaving daarvan), zelfregulering (waar mogelijk), technische filters en voorlichting.

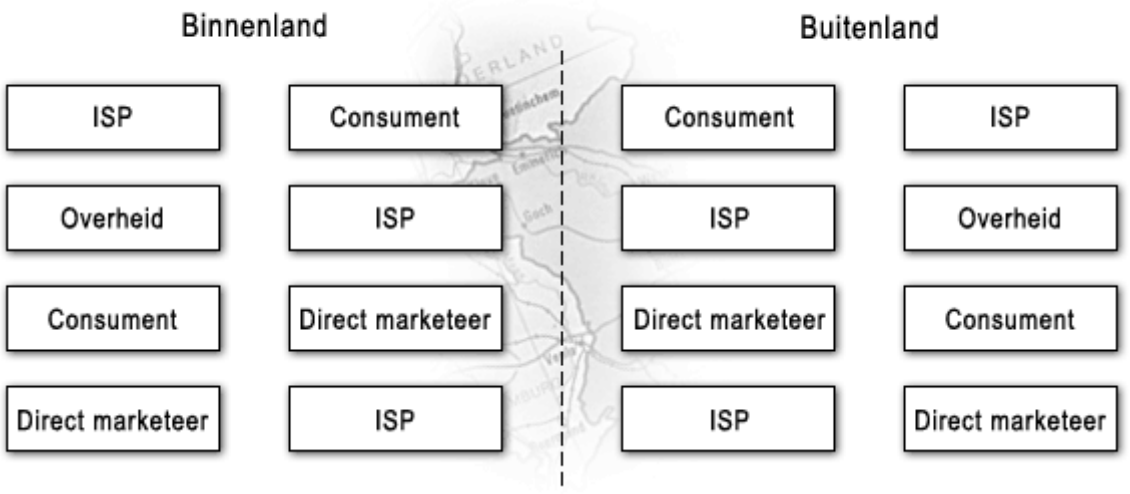
In dit hoofdstuk staat grensoverschrijdende, internationale samenwerking centraal. Aan de hand van de theoretische noties uit hoofdstuk drie wordt gepoogd om handvatten te bieden voor het forceren van die samenwerking. Wat in de gewijzigde verhoudingen van de netwerkmaatschappij de rol van de overheid kan zijn, wordt hier eveneens nader belicht.

Nu is gebleken dat de actoren die bij spambestrijding betrokken zijn nog veel verschillende belangen en percepties hebben met betrekking tot de spamproblematiek, is het nuttig om de conclusies van het falen van gezamenlijke spambestrijding uitgaande van de

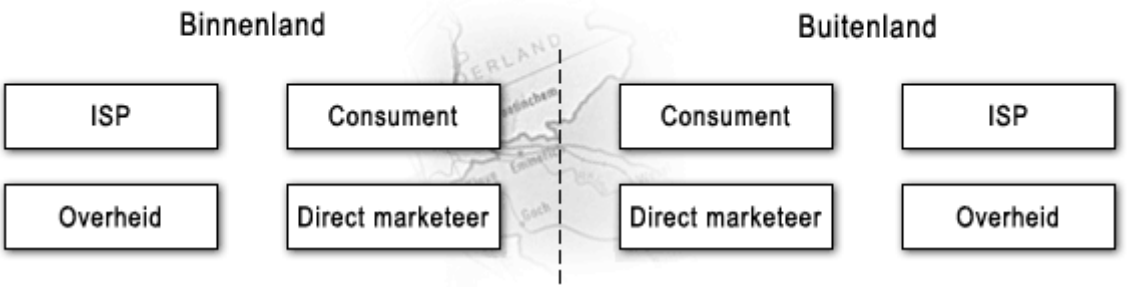
netwerkbenadering nog eens op een rijtje te zetten. Wat zijn nu de bouwstenen om spambestrijding tot een groter succes te maken? Hoe kan netwerkmanagement toegepast worden om de betrokken actoren op één lijn te krijgen?

Op de volgende pagina's is zichtbaar wat de situatie met betrekking tot spambestrijding nu is, hoe die zou zijn als de belangrijkste betrokken actoren op nationaal niveau intern zouden samenwerken (dus bijvoorbeeld de NLIP als brancheorganisatie van de Nederlandse ISP's), hoe het zou zijn als die interne samenwerking tot contacten leidt met de andere actoren in een nationale omgeving en ten slotte wat de ideale situatie is: als de koepelorganisaties van de betrokken actoren zouden samenwerken zonder rekening te houden met landsgrenzen.

Huidige situatie

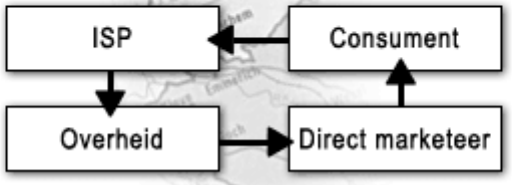


Interne samenwerking op nationaal niveau



Externe samenwerking op nationaal niveau

Externe samenwerking op internationaal niveau



De kern van de faalfactoren is dat de onzekerheid nog te groot is over inhoud, instituties en strategie. Koppenjan en Klijn formuleerden in hun *'Managing Uncertainties in Networks'* de te volgen strategie om de juiste keuze te maken om die onzekerheden te reduceren (zie ook hs 3).[109] Hun betoog valt in drie delen uiteen, waarvan dit de meest relevante factoren zijn:

[109] Koppenjan, J.F.M. en Klijn, E.H (2004) Blz. 249-256

Dialoog creëren door: (inhoud)	- het stellen van gemeenschappelijke doelen - variëteit creëren om fixatie te voorkomen - procesafspraken te maken in plaats van over inhoud te discussiëren - duidelijke criteria af te spreken
Regels afspreken door: (instituties)	- een arbiter aan te stellen - af te spreken welke actoren worden toegelaten - een beloningsstructuur af te spreken
Gemeenschappelijk referentiekader creëren door: (strategie)	- de condities voor samenwerking aan te scherpen

Wat in het bovenstaande schema echter ontbreekt is de bindende factor. Om de onzekerheden te reduceren moeten de condities voor samenwerking worden aangescherpt. Tevens moet er worden gewerkt aan gezamenlijke beeldvorming over het probleem door middel van facilitering van het proces, of arbitrage in het proces. Maar wie brengt nu de betrokken actoren samen, opdat de dialoog gestart kan worden, de regels van het spel geformuleerd kunnen worden en er uiteindelijk een gemeenschappelijk referentiekader ontwikkeld kan worden?

6.2 Het aanstellen van een facilitator, het instellen van een instituut

Het antwoord op deze vraag was de facilitator of *game manager*. Die moet ervoor zorgen dat het proces op gang komt, op gang wordt gehouden en dat de samenwerking duurzaam is. Hij moet arena's aan elkaar koppelen, de agenda bijhouden, expertise regelen,

knelpunten signaleren en voortdurend de gang van zaken evalueren. En om ervoor te zorgen dat de andere actoren hem accepteren, moet hij neutraal zijn, vertrouwen opwekken, gezag uitstralen en competent zijn.

De noodzaak van een facilitator is te koppelen aan de noodzaak van een grensoverschrijdend instituut dat de bevoegdheid heeft om voor aangesloten lidstaten bindende afspraken op te stellen. En zo kom ik toch weer uit op een instantie als de Verenigde Naties. Het is waarschijnlijk eenvoudiger om een bestaand instituut, dat qua inrichting en werking reeds gelijkenis vertoont met de organisatie waar ik nu naar zoek, een extra taak te geven, dan een geheel nieuw instituut op te richten. Het is maar een voorbeeld van het soort organisatie wat nodig zou zijn om spam effectief te bestrijden. Als de betrokken actoren liever een geheel nieuw instituut oprichten, dan is dat natuurlijk alleen maar aan te moedigen, vooral als dat een gezamenlijk standpunt is. Maar uitgaande van dit voorbeeld zouden de VN de WIPO kunnen gebruiken als het onderdeel van de organisatie dat als facilitator op het gebied van spambestrijding kan optreden. De WIPO kan hier een neutrale positie innemen en tegelijkertijd een platform bieden voor de totstandkoming van grensoverschrijdende wet- en regelgeving. De bij de WIPO aangesloten lidstaten beslissen dan volgens het intergouvernementele principe (er moet een unaniem besluit komen) welke wet- en regelgeving zij willen.

Het is natuurlijk wenselijk dat de unanimiteitseis wordt vervangen door een simpele meerderheidseis of een variant daarop. Maar de kans dat dat zal gebeuren is vrij groot indien de eerste stap wordt gezet om de WIPO te gaan gebruiken voor wet- en regelgeving op het gebied van spambestrijding. Waarom is dat? Welnu, een belangrijk punt bij deze oplossing is dat de netwerkbenadering er in beginsel van uitgaat dat samenwerking noodzakelijk is in een netwerksituatie waarbij de actoren wederzijds van elkaar afhankelijk zijn door de horizontalisering van relaties, waarbinnen hiërarchische sturing problematisch zo niet onmogelijk wordt. Top-down sturing kan niet (langer), dus moet er samenwerking komen. Maar wat in de praktijk juist vaak opvalt is dat die samenwerking veelal tot stand komt met als doel om weer een nieuwe top, een nieuw centrum te creëren. Dat is een opvatting die min of meer indruist tegen de gangbare

opvattingen over netwerken, zoals bijvoorbeeld deze: “*We moeten voorbij aan het model van de piramide, aan het idee dat deze samenleving een centrum zou hebben, aan het idee dat dat centrum de nationale wetgever zou zijn.”*[110]

De constatering dat de betrokken actoren wederzijds van elkaar afhankelijk zijn in het komen tot een oplossing betekent niet per definitie dat er geen enkele sprake van centrale sturing kan zijn. Bij spambestrijding blijkt namelijk dat centrale sturing weliswaar niet aanwezig is omdat er geen grensoverschrijdend instituut is dat de bevoegdheid heeft om te kunnen sturen, maar de wil vanuit de andere actoren (behalve de direct marketeers) om een actor aan te wijzen die op dit gebied gezaghebbend is, is wel degelijk aanwezig. De vingers wijzen dan in de richting van ‘de overheid’, waarbij het ook bij de betrokken actoren zelf onduidelijk is welke overheid dat dan moet zijn. Een overheid met grensoverschrijdende bevoegdheden, zoveel is duidelijk. Maar zoals gezegd: zo’n instituut bestaat niet en spambestrijding moet toch vooral een samenspel van actoren zijn, daar de beschikbare maatregelen complementair zijn.

En dan zijn de VN als platform voor samenwerking dus een mogelijke oplossing. Het voorbeeld wat hier analoog aan is, is de Europese Unie. Ook daar wordt samenwerking als noodzakelijk gezien om tot oplossingen te komen voor problemen die grensoverschrijdend zijn. Maar ook daar mondt die samenwerking in de praktijk uit in het overdragen van bevoegdheden van de aangesloten lidstaten naar het supranationale niveau. Er is dan in feite sprake van een spill-over van effecten. Eerst wordt de (relatief kleine) stap gezet om samen te gaan werken, vervolgens wordt er feitelijk vanuit de overweging dat als er dan toch samengewerkt wordt, het makkelijker zou zijn om het beleid aan dat hogere niveau over te laten, besloten om de bevoegdheden daadwerkelijk aan dat hogere niveau over te dragen.

[110] Frissen, P.H.A. (1993)

Overigens ging ik er toen ik aan deze scriptie begon van uit dat het aanstellen van een facilitator zinloos was. Er was immers te weinig grensoverschrijdend overleg tussen de betrokken actoren, waardoor de 'dialogue of the deaf' waar Koppenjan en Klijn het over hebben dusdanig sterk is, dat er van samenwerking in het geheel geen sprake is. Er zou in die redenatie niemand zijn die een facilitator aan zou willen stellen (of het zelf zou willen worden). De stap van het in woord belijden van een noodzakelijke verandering naar het daadwerkelijk iets doen zou te groot zijn. Maar van die gedachte ben ik inmiddels genezen. Er zit wel degelijk progressie in de opvattingen van de betrokken actoren over spambestrijding, maar het is vooral de grensoverschrijdende stap die nog ontbreekt. Door de spill-over effecten van die steeds verdergaande ontwikkelingen op spambestrijdingsgebied is mijn verwachting dat er wel degelijk een facilitator zal worden aangesteld en dat er een grensoverschrijdend instituut zal worden ingesteld als het besef van de noodzaak daartoe nog verder toeneemt.

6.3 Obstakels verwijderen

Vooraleer er een facilitator en grensoverschrijdend platform gekozen worden is het noodzakelijk om eerst eens te kijken hoe een overlegorgaan waarbinnen overheden (nationale staten), ISP's, direct marketeers, consumentenorganisaties en het bedrijfsleven om de tafel gaan zitten –begeleid door een facilitator- de overige obstakels überhaupt uit de weg kan ruimen. Om terug te gaan naar de vraag uit paragraaf 6.1: Hoe kan een (beter) gemeenschappelijk referentiekader ontwikkeld worden?

De problemen die naast het ontbreken van een grensoverschrijdend platform eerder vastgesteld waren met betrekking tot de positie van de actoren in het spambestrijdingsnetwerk waren:

1. de onzekerheden zijn nog te groot
2. er is wel een gemeenschappelijk referentiekader (spam moet bestreden worden), maar binnen dat kader lopen de meningen nog te veel uiteen
3. er is geen sprake van bewuste of opzettelijke geslotenheid van actoren, maar de meeste actoren handelen nog niet echt open
4. er is onvoldoende besef aanwezig dat de actoren bij spambestrijding wederzijds van elkaar afhankelijk zijn

De aanpak

Door het stellen van een gemeenschappelijk doel kunnen onzekerheden worden gereduceerd. Dat doel is in de kern: spam moet bestreden worden. De discussie over de exacte probleemdefinitie van spam (opt-in versus opt-out, is alleen commerciële e-mail spam of is alle ongevraagde e-mail dat?) leidt echter in de praktijk tot impasses en verwarring. Om dit niet tot een beletsel tot samenwerking te laten worden is een oplossing om bij het overleg tussen de verschillende actoren afspraken te maken over het proces in plaats van te discussiëren over de inhoud. Het vaststellen van inhoudelijke criteria kan in een later stadium nog, als de betrokken actoren meer weten over elkaars standpunten, posities en belangen zodat zij daar wellicht beter rekening mee kunnen en willen houden. De onzekerheden op het inhoudelijke gebied worden zo hopelijk tijdig geneutraliseerd.

Op strategisch gebied moeten de condities voor samenwerking worden aangescherpt. Druk van buitenaf om snel tot een oplossing te komen kan hierbij helpen. De economische kosten van spam zullen hier waarschijnlijk doorslaggevend in zijn. Zodra die echt te hoog worden voor de betrokken actoren, dan zal de druk toenemen en vallen strategische belemmeringen weg. Free-rider gedrag is dan te voorkomen door een beloningsstructuur af te spreken. Of het omgekeerde: actoren kunnen beboet worden indien zij niet meehelpen met het zoeken naar een gezamenlijke oplossing. Om dit te beoordelen kan een arbiter worden aangesteld.

Maar negatieve sancties zijn in beginsel onwenselijk. Het spel bestaat uit overleg, overtuiging, onderhandelen en slechts als het echt niet anders kan uit machtsuitoefening. Het is wenselijker om de oplossing voor conflicten te zoeken in één van die eerste drie oplossingen. Een arbiter kan hierbij helpen, of er kan bijvoorbeeld een externe adviseur worden ingeschakeld die een frisse blik op het proces kan werpen. De doeltreffendheid van de uiteindelijke oplossing is afhankelijk van de mate van samenwerking en die is optimaal als er zo weinig mogelijk frictie bestaat.

De geslotenheid van actoren die niet bewust of opzettelijk aanwezig is kan verder gereduceerd worden door simpelweg de discussie met de andere actoren over de spamproblematiek aan te gaan. Dat gebeurt ook al wel, er is geen sprake van fixatie op de eigen standpunten. Dit is bijvoorbeeld te zien in de opschuivende opvattingen van minister Brinkhorst over de beste aanpak van spambestrijding (zie paragraaf 4.4). Externe adviseurs , aanjagers of een arbiter kunnen ook hier een rol spelen in het nader tot elkaar brengen van de betrokken actoren.

Gecombineerd kunnen de effecten van deze maatregelen uitgroeien tot een breed gedragen gemeenschappelijk referentiekader, op basis waarvan dan gehandeld kan worden in een poging het spamprobleem te elimineren.

6.4 De rol van de overheid

Maar wie stelt nu die facilitator aan en wie bepaalt nu wat het grensoverschrijdende platform wordt waarbinnen spambestrijding aan de orde zal worden gesteld? In het paragraaf 6.2 ben ik er impliciet al van uitgegaan dat nationale staten hier een grote rol in spelen, zeker als het gaat om wet- en regelgevende bevoegdheden. Paragraaf 6.3 concludeerde hetzelfde: want wet- en regelgeving zijn juist datgene wat nog in grote mate ontbreekt in de aanpak van spambestrijding. Dat feit, gecombineerd met de overige actoren die ook

allemaal naar ‘de overheid’ wijzen als de centrale actor (!) die sturing moet geven bij de aanpak van spam, leidde tot het kijken naar een grensoverschrijdend instituut met de bevoegdheid om wet- en regelgeving op te stellen. Dat in de gekozen oplossing -de VN als voorbeeld van het benodigde type organisatie- ook direct een facilitator gevonden is die voldoet aan de eisen die aan een facilitator gesteld worden, is een voordeel.

Dat neemt niet weg dat het niet per se een overheidsinstantie moet zijn die de rol van facilitator op zich neemt. Een onafhankelijk bureau zou dit ook kunnen doen, mits de betrokken actoren vinden dat deze aan de eisen die aan een facilitator gesteld worden voldoet. Het grensoverschrijdende platform dat noodzakelijk is om met name supranationale wet- en regelgeving te realiseren kan echter wel alleen door overheden ingesteld worden. Alleen zij hebben de bevoegdheid om dit te doen. ISP’s, direct marketeers, het bedrijfsleven en consumentenorganisaties zijn niet democratisch gelegitimeerd om wet- en regelgeving vast te stellen. Zelfs in een wereld die zich steeds meer kenmerkt door globalisering blijven natiestaten wat dat betreft nog een vrijwel onverminderd belangrijke rol spelen.

De overheid kan dus als facilitator optreden en is eveneens in staat om door middel van internationaal overleg tussen nationale staten te komen tot een instantie die de bevoegdheid heeft om grensoverschrijdende maatregelen te nemen met betrekking tot spambestrijding. In een minder neutrale positie als regisseur kan de overheid ook een rol spelen in het besluitvormingsproces:

> *‘The government could award authoritative value to the relevant social constructions. The orchestrating role, the continuous guiding of solution trajectories and problem flows, implies judging various administrative, professional and social initiatives in the light of the problems that political actors want solved.’.*[111]

[111] Teisman, G.R. (1997)

In dit geval is er echt sprake van centrale sturing vanuit de overheid. Zowel bij een neutrale positie als facilitator als bij een meer sturende positie als regisseur kan hetzelfde effect worden bereikt bij spambestrijding. De overheid kan ondanks de beperkingen die aan haar sturende rol zijn opgelegd in de steeds complexer wordende maatschappij zowel inhoudelijk als procesmatig randvoorwaarden creëren en als aanjager functioneren van bredere en diepere samenwerking tussen actoren.[112] De voorwaarden voor succes blijven hetzelfde: de aanpak moet grensoverschrijdend zijn en moet alle mogelijke spambestrijdingsmaatregelen aan elkaar koppelen om optimaal effectief te zijn. De uiteindelijke keuze tussen deze varianten is een politieke keuze, maar gebaseerd op de bevindingen uit de voorgaande hoofdstukken zal ik het niet nalaten om een (normatieve) aanbeveling te doen in het volgende hoofdstuk.

6.5 Symptoombestrijding?

De conclusie van dit schrijven is dat spambestrijding een gezamenlijke aanpak vereist en dat alleen onder die voorwaarde het kwaad (spam) zoveel mogelijk kan worden ingedamd. Of met een gezamenlijke aanpak spambestrijding waterdicht zal zijn, is voorlopig onbekend. Waarschijnlijk blijft er gedurende lange tijd een kat-en-muis spelletje tussen spammers en spambestrijders bestaan, waarbij er steeds nieuwe methoden worden gevonden om te spammen of juist om spam te weren.

Maar ongeacht de vraag of spam definitief de wereld uitgeholpen kan worden, is de vraag die al die tijd bij mij is blijven knagen en die nog steeds open blijft staan, of spambestrijding niet slechts symptoombestrijding is. Spam veroorzaakt immers niet alleen de problemen waarvoor ik in deze scriptie heb geprobeerd om oplossingen voor te verzinnen, maar het is zelf ook een gevolg van een

[112] Heuvelhof, In' t Veld & De Bruijn (2002)

ander probleem, wat in hoofdstuk drie aan bod gekomen is als achterliggende oorzaak van het spamprobleem. Deterritorialisering was daar het centrale begrip.

Hoe zat het ook alweer: Steeds meer activiteiten zijn grensoverschrijdend. Door ICT-ontwikkelingen zijn begrippen als ‘afstand’ en ‘tijd’ een wezenlijke andere rol gaan spelen. Veel activiteiten kunnen dankzij ICT wereldwijd worden ontplooid, onafhankelijk van de geografische locatie. De afnemende binding aan een bepaald grondgebied heeft onvermijdelijke gevolgen voor het handelingsvermogen van de nationale staat, door de het gebonden zijn van instrumenten aan territoriale grenzen. Wet- en regelgeving is immers onlosmakelijk aan territoir gebonden.

Spam is een voorbeeld van een grensoverschrijdende activiteit. Het is een activiteit met vooral negatieve gevolgen, de financiële opbrengsten voor de spammer daargelaten. Net als bij terrorisme is ‘de vijand’ ongrijpbaar, hij kan uit kleine cellen bestaan en hij kan zich makkelijk verplaatsen. In tegenstelling tot bij terroristische aanslagen echter, die veelal bestaan uit aanslagen op personen en gebouwen, kan bij spam de dader zich zelfs virtueel verplaatsen. Niet de fysieke ruimte, maar de virtuele ruimte is het speelveld van de spammer. En over deze virtuele ruimte is nog maar weinig bekend. De handvatten in deze scriptie zijn slechts relevant in het bestrijden van de gevolgen van spam, maar de oorzaak van het bestaan van spam wordt feitelijk slechts aangestipt. Aan oplossingen voor het onderliggende probleem kom ik in het geheel niet toe.

Met deze scriptie is slechts een begin gemaakt met het kijken naar de effecten van deterritorialisering die de WRR in 1998 voorspelde. Spam is hier een gevolg dat in de praktijk is opgetreden. Maar meer onderzoek naar de gevolgen van deterritorialisering en met name ook de betekenis voor de inrichting en werking van de virtuele ruimte is mijns inziens gewenst. Want niet alleen bij spam en terrorisme speelt de afnemende binding aan een bepaald grondgebied een rol, maar ook bijvoorbeeld bij zaken als virusbestrijding (momenteel een *hot issue* op internetgebied) en fiscaal recht:

‘Dat geldt ook voor het fiscale recht. Naarmate handelingen meer langs elektronische weg plaatsvinden maken goederen plaats voor diensten en wordt de fysieke aan geografische grenzen gebonden locatie minder relevant. Zoals gezegd komt de handhaving van de belastinginning onder druk te staan omdat het huidige stelsel van belastingheffing is gebaseerd op het bestaan van staten en geografische grenzen. Zo wordt bijvoorbeeld inkomstenbelasting en omzetbelasting geheven in, respectievelijk, het land waar het inkomen wordt genoten en het land waar de verkoop van goederen plaatsvindt.’[113]

Er zijn pas een paar kleine stappen gezet wat betreft het in kaart brengen van de virtuele ruimte, maar er is nog bijna letterlijk een –virtuele- wereld te winnen.

[113] Prins, J.E.J. (1999)

Hoofdstuk 7
Conclusies & Aanbevelingen

7.1 Waarom spam een probleem is

De doelstelling van deze scriptie was om te analyseren wat anno 2004 de problemen zijn met betrekking tot spambestrijding en hoe overheden met spambestrijding omgaan. Uit deze analyse moesten conclusies en aanbevelingen volgen om spambestrijding waar mogelijk effectiever te laten verlopen. De centrale vraagstelling hierbij was: Kan de overheid een rol spelen bij spambestrijding, en zo ja: voor welke overheid is welke rol weggelegd?

In dit afsluitende hoofdstuk staat beschreven wat die problemen bij spambestrijding precies zijn en hoe ik uiteindelijk tot het antwoord op die centrale vraagstelling ben gekomen.

De gevolgen van spam

Ik begon deze scriptie met de stelling dat spam een probleem is. De sociale en economische kosten van spam zijn hoog, het belemmert de informatie uitwisseling op internet en het maakt inbreuk op de privacy van de ontvanger.

Om spam te kunnen bestrijden is het noodzakelijk om te weten hoe e-mail precies werkt en hoe het technische proces achter spam precies in elkaar steekt. Spam blijkt door de ontvanger niet eenzijdig af te stoppen, want dankzij de technische onvolkomenheden van e-mail zijn spammers in staat om door middel van talloze technische trucs hun spam e-mails af te blijven leveren bij honderden

miljoenen internetters. Daarnaast is het relatief eenvoudig om spam te versturen. Een computer en een internetaansluiting zijn voldoende om wagonladingen ongewenste e-mail te versturen. En het verzamelen van de benodigde e-mailadressen is eenvoudig: op internet zijn voor een appel en een ei cd's te koop met miljoenen e-mailadressen.[114]

Technische filters die internetgebruikers installeren om spam te weren volstaan niet, maar wet- en regelgeving die het versturen van spam verbiedt, is ook geen afdoende maatregel om spam te bestrijden. De spammer is namelijk in staat om zijn fysieke locatie te camoufleren door bijvoorbeeld het afzenderadres te vervalsen of door de spam door middel van gehackte pc's van andere gebruikers te versturen. Alleen als dit niet gebeurt of als de spammer zijn geld op gaat halen, is het mogelijk om hem te pakken te krijgen.

En er is nog een probleem bij die wet- en regelgeving. Actoren hanteren verschillende percepties over de definitie van spam. De ontvanger van spam wil er niets mee te maken hebben, de verzender ziet het juist als zijn broodwinning. Internetproviders, consumenten(organisaties), bedrijfsleven en direct marketeers hanteren ieder een eigen definitie van spam. Om aan alle eisen van die actoren tegemoet te komen zou in de definitie van spam rekening gehouden moeten worden met commercieel gedrag, de psychologie van de ontvanger, de juridische context, economische overwegingen en technische belemmeringen en mogelijkheden. Het is bijna onmogelijk om een definitie te hanteren die al deze elementen bevat.

Spam als gevolg

Als je nog verder de diepte ingaat, dan zie je dat spam niet alleen problemen veroorzaakt, maar zelf ook het gevolg is van een ander probleem. Wat met de reeds eind 19e eeuw ingezette industriële revolutie begon is nu uitgemond in de informatie revolutie, ook wel

[114] Zie bijlage C

ICT-revolutie genoemd, omdat die twee zo onlosmakelijk met elkaar verbonden zijn. De ICT-ontwikkelingen van de afgelopen decennia hebben grote gevolgen voor de samenleving gehad. Deterritorialisering is hier het centrale begrip. Door ICT-ontwikkelingen zijn begrippen als ‘afstand’ en ‘tijd’ een wezenlijke andere rol gaan spelen. Veel activiteiten kunnen dankzij ICT wereldwijd worden ontplooid, onafhankelijk van de geografische locatie. De afnemende binding aan een bepaald grondgebied heeft ‘onvermijdelijke gevolgen voor het handelingsvermogen van de nationale staat’, door de gebondenheid van instrumenten aan territoriale grenzen. Zo is wet- en regelgeving onlosmakelijk aan territoir gebonden.

Door het verdwijnen van grenzen is de staat niet langer de enige gezaghebbende structuur in de maatschappij. Grensoverschrijdende activiteiten vereisen (wereldwijde) samenwerking in steeds horizontalere netwerken. De veranderende gezagsverhoudingen in deze netwerken leiden tot een nieuw soort, veelal uiterst complexe, problemen (wicked problems) die vaak om een nieuw soort oplossingen vragen. Het is hierbij bovenal duidelijk dat eenzijdige actie van actoren niet effectief is. Interactie met andere actoren is noodzakelijk, doordat in netwerken wederzijdse afhankelijkheden zijn ontstaan.

Spam is een voorbeeld van een gevolg van deterritorialisering. Spammers zijn onafhankelijk van een geografische locatie om hun activiteiten te ontplooien, daar zij van het internet gebruik maken. Het internet heeft geen hiërarchisch karakter en is grensoverschrijdend. De maatregelen om spam te bestrijden zouden daarom net als spam zelf grensoverschrijdend moeten zijn om effectief te kunnen zijn. Samenwerking tussen nationale staten lijkt derhalve onvermijdelijk om tot een oplossing van het spamprobleem te komen. De bij spambestrijding betrokken actoren zijn wederzijds van elkaar afhankelijk in het komen tot een oplossing. Dit geldt zowel voor het definiëren van een gezamenlijke probleem- en doelstelling als om de grensoverschrijdende samenwerking te realiseren. In deze netwerksituatie is het ontwikkelen van een gemeenschappelijk referentiekader derhalve van belang.

Er zijn een aantal voorwaarden waar aan voldaan moet worden om dat gemeenschappelijke referentiekader te ontwikkelen. De actoren in het netwerk moeten zich er van bewust zijn dat ze van elkaar afhankelijk zijn bij het bereiken van hun doelen, ze moeten openstaan voor de belangen en percepties van andere actoren in het netwerk en ze moeten beseffen dat die andere actoren elk hun eigen achtergrond hebben. Dit besef kan gerealiseerd worden door een aantal strategieën te volgen om de onzekerheid over de te volgen strategie, over de inhoud en instituties te reduceren. Het gaat dan om het streven naar gezamenlijke doelen, het creëren van variëteit om fixatie te voorkomen, het maken van procesafspraken in plaats van te discussiëren over de inhoud, het afspreken van duidelijke criteria, het aanstellen van een arbiter, het maken van afspraken over toe te laten actoren, het afspreken van een beloningsstructuur en het aanscherpen van de condities voor samenwerking.

Door de wederzijdse afhankelijkheid van actoren kan een netwerkmanager in dit proces geen centrale bestuurder of regisseur zijn, maar veeleer een bemiddelaar en stimulator. Kortom: het spel heeft een facilitator of een *game manager* nodig. Die moet ervoor zorgen dat het proces op gang komt, op gang wordt gehouden en dat de samenwerking duurzaam is. Hij moet arena's aan elkaar koppelen, de agenda bijhouden, expertise regelen, knelpunten signaleren en voortdurend de gang van zaken evalueren. En om ervoor te zorgen dat de andere actoren hem accepteren, moet hij neutraal zijn, vertrouwen opwekken, gezag uitstralen en competent zijn.

7.2 Waarom samenwerking bij spambestrijding faalt

Na de constatering dat samenwerking noodzakelijk is en het in kaart brengen van de voorwaarden voor die samenwerking stelde ik de vraag waarom we dan nog steeds last hebben van spam? Is die noodzakelijke samenwerking er dan niet? Wat wordt er eigenlijk gedaan om spam te bestrijden?

De meest gebruikte praktische methode om spam te bestrijden is het gebruik maken van technische filters. Er is een heel scala aan filters op de markt, maar elk heeft zo zijn eigen onvolkomenheden waardoor gewone e-mail als spam wordt aangemerkt ('false positives') of spam e-mail toch wordt afgeleverd ('false negatives'). Als economische maatregelen zijn boetes en micropayments inzetbaar. Maar spammers zijn nauwelijks te traceren en ze kunnen 'virtueel' spammen vanuit landen waar spam (nog) niet verboden is en daardoor werken boetes nauwelijks. Micropayments blijken eveneens geen praktische oplossing. Zowel verzender als ontvanger zou mee moeten doen met het systeem, legitieme massamailers worden onevenredig zwaar belast, het idee van internet als gratis, openbaar, wereldwijd communicatiemedium zou ten gronde gaan als er voor elke e-mail betaald zou moeten worden en het benodigde globale online geldtransfersysteem bestaat vooralsnog niet eens.

Het aantal juridische maatregelen tegen spam neemt nog steeds toe, maar het aantal spam e-mails is nog niet verminderd. Toch is de hoop van veel spambestrijders op wet- en regelgeving gericht. Dat de mazen in de wet vrijwel overal nog erg groot zijn, betekent niet dat er in het geheel geen ontwikkeling in zit. Wet- en regelgeving wordt als noodzakelijk gezien om spambestrijding effectief te laten zijn, maar niet als hét wondermiddel. Met name voor legitieme bedrijven en personen is wet- en regelgeving wel degelijk relevant. Al is het maar voor het rechtvaardigheidsgevoel van de ontvanger van spam. De communicatieve aanpak staat nog in de kinderschoenen. Voorlichting (ook wel het creëren van 'user-awareness' genoemd) wordt als relevant gezien om spam te voorkomen, maar wie deze taak op zich moet nemen is een punt van voortdurende discussie. Zelfregulering ten slotte faalt in de praktijk omdat de meeste spammers ronduit crimineel zijn en zich nergens aan willen binden, dus ook niet aan een brancheorganisatie die zelfregulering op het oog heeft.

Toch zijn dit de enige mogelijkheden die voorhanden zijn om het spamprobleem te bestrijden. De meest optimale oplossing van het spamprobleem lijkt dan ook een combinatie van al deze maatregelen te zijn om een zo groot mogelijk front te vormen tegen spammers. Zo kunnen overheden bijvoorbeeld een juridisch kader scheppen, waarna de markt vervolgens probeert door middel van zelfregulering en technische filters de excessen uit te bannen die er dan nog zijn. Samenwerking tussen de verschillende betrokken actoren om alle vormen van spambestrijding inhoudelijk op elkaar aan te laten sluiten is derhalve noodzakelijk, maar vooralsnog afwezig.

Actoren, belangen en percepties

De methoden van spambestrijding zijn dus niet op elkaar afgestemd. De volgende stap was dan ook het in kaart brengen wie nu precies de betrokken actoren zijn en wat hun belangen en percepties zijn. Is er sowieso wel sprake van interactie of zitten alle actoren in verschillende netwerken die niet of niet voldoende aan elkaar verbonden zijn? Hoe definiëren actoren ‘spam’? Waar worden de beslissingen over spambestrijding genomen? In welke arena’s? En zijn die aan elkaar gekoppeld? In hoeverre zijn de actoren van elkaar afhankelijk in het bereiken van hun doelen? Kortom: wordt er bij spambestrijding voldaan aan de voorwaarden die de netwerkbenadering stelt aan een succesvolle manier van het benaderen van een beleidsproces of is de praktijk weerbarstiger?

De samenwerking bij spambestrijding blijkt nog niet voldoende van de grond te komen door een aantal factoren. Ten eerste zijn de onzekerheden over inhoud, instituties en strategie nog te groot. Ten tweede er is wel een gemeenschappelijk referentiekader (spam moet bestreden worden), maar binnen dat kader lopen de meningen nog te veel uiteen. Ten derde zijn er nauwelijks blokkades voor interactie en zelfs top-down sturing zou mogelijk zijn, maar er ontbreekt een instituut waarbinnen die interactie en sturing plaats kunnen vinden. Ten vierde is er geen sprake van bewuste of opzettelijke geslotenheid van actoren, maar de meeste actoren handelen nog niet echt open. Hetgeen weer te maken heeft met het vijfde punt: het onvoldoende aanwezige besef dat de actoren bij spambestrijding wederzijds van elkaar afhankelijk zijn.

In een netwerksituatie worden de grenzen van het spel bepaald door de onderlinge verhoudingen. Die zijn in principe goed, er is een gemeenschappelijke vijand (de spammer) alleen is de coalitie van de ‘good guys’ nog niet helder gedefinieerd door de actoren zelf.

Indien er wordt gekozen voor (onder andere) een juridische oplossing, werkt samenwerking vaak niet door de onzekerheid over de definitie van spam en de daardoor complexe wet- en regelgeving door onder andere de voortdurende discussie over opt-in of opt-out oplossingen. Het gaat dan niet zozeer over onwil bij overheden, maar het inzicht ontbreekt vaak gewoon. De verschillen in de bestuurlijke en politieke systemen tussen nationale staten vormen hierbij een extra belemmering. En zelfs relatief onbelangrijk lijkende factoren als afstand en taal- en cultuurverschil kunnen obstakels vormen. En zo hebben al deze factoren tezamen tot gevolg dat er van een echte, serieuze grensoverschrijdende aanpak van de spamproblematiek geen sprake is.

De kern van het verhaal lijkt te zijn dat actoren feitelijk niet over een en hetzelfde probleem spreken, want ieder definieert spam anders. En zelfs als er wel overeenstemming over het probleem is, dan is er nog geen eenduidige manier om het aan te pakken. Dat is echter niet hetzelfde als stellen dat er bij een ‘modern’ probleem als spam geen oplossingen meer mogelijk zijn, er zal soms alleen op nieuwe manieren gepoogd moeten worden om tot oplossingen te komen. Voor overheden betekent dit meer dan voorheen het zoeken naar samenwerkingsverbanden in plaats van het simpelweg opleggen van nieuwe regels.

7.3 Hoe moet het dan wel?

En zo komen we bij de vraag hoe die samenwerking georganiseerd moet worden. Als het proces naar meer samenwerking gefaciliteerd moet worden, om zo de onzekerheden te reduceren die bij actoren over elkaar en over de spambestrijdingsmethoden bestaan, dan is het aanstellen van een facilitator een oplossing. Dat wet- en regelgeving juist datgene zijn wat nog in grote mate

ontbreekt in de aanpak van spambestrijding, gecombineerd met het feit dat de betrokken actoren allemaal naar ‘de overheid’ wijzen als de centrale actor (!) die sturing moet geven bij de aanpak van spam, leidde tot het zoeken naar een supranationale organisatie die bevoegd zou zijn om grensoverschrijdende maatregelen te nemen tegen spam. Dit moet wel een overheidsvorm zijn, daar andere actoren niet democratisch gelegitimeerd zijn om wet- en regelgeving vast te stellen.

En dan is de Verenigde Naties een voorbeeld van het type organisatie dat nodig is om spam effectief te kunnen bestrijden. Uitgaande van dit voorbeeld zouden de VN de WIPO kunnen gebruiken als het onderdeel van de organisatie dat als facilitator op het gebied van spambestrijding kan optreden. De WIPO kan hier een neutrale positie innemen en tegelijkertijd een platform bieden voor de totstandkoming van grensoverschrijdende wet- en regelgeving. De bij de WIPO aangesloten lidstaten beslissen dan volgens het intergouvernementele principe (er moet een unaniem besluit komen) welke wet- en regelgeving zij willen.

De verwachting is dat dit soort grensoverschrijdende samenwerking uiteindelijk uitmondt in het overdragen van bevoegdheden van de aangesloten lidstaten naar het supranationale niveau. Er is dan in feite sprake van een spill-over van effecten. Eerst wordt de (relatief kleine) stap gezet om op een functioneel niveau samen te gaan werken, vervolgens wordt er feitelijk vanuit de overweging dat als er dan toch samengewerkt wordt, het makkelijker zou zijn om het beleid aan dat hogere niveau over te laten, besloten om de bevoegdheden daadwerkelijk aan dat hogere niveau over te dragen. Nationale staten hevelen slechts een aantal functionele elementen over naar het supranationale niveau (harmonisatie) en houden op die manier hun soevereiniteit zo goed mogelijk in stand.

De stap die daarna nog gezet moet worden is die van regelgeving naar handhaving. Dat moet namelijk ook de grens over en vereist dus wereldwijde samenwerking tussen opsporingsorganisaties.

Effectieve spambestrijding kan en zal echter niet alleen vanuit de overheid kunnen komen. Ook het bedrijfsleven speelt een belangrijke rol. De grote overlast die spam veroorzaakt heeft, heeft geleid tot een groot aanbod van technische bestrijdingsmaatregelen op de (digitale) markt. Ook hier ontbreekt samenwerking echter, zoals we eerder gezien hebben. De meest effectieve (lees: optimale) vorm van technische filtering wordt hierdoor dus niet bereikt. Economische motieven (bedrijfsgeheimen van spamfilter bouwers die de concurrent niet willen informeren over de door hen gebruikte technieken) spelen hier een grote rol.

Aanbevelingen

Zoals aangekondigd in hoofdstuk zes zal ik hier enige aanbevelingen doen gebaseerd op mijn voorgaande conclusies. De aanbeveling aan bijvoorbeeld de Nederlandse overheid, bij spambestrijding met name vertegenwoordigd door de ministers van Economische Zaken en Justitie, maar met als eindverantwoordelijke uiteindelijk de regering, is dan ook om er bij de Europese Commissie op aan te dringen om op zoek te gaan naar samenwerking die ook over de grenzen van de Europese Unie heen gaat. In zijn algemeenheid geldt dat om effectieve maatregelen te kunnen nemen overheden wereldwijd aangemoedigd moeten worden om supranationale organen en overlegplatformen op te zoeken om vanuit dat uitgangspunt de strijd met spam aan te gaan. En als toevoeging op deze aanbeveling zou er dan direct gewezen kunnen worden op de WIPO als mogelijk instituut waarbinnen deze grensoverschrijdende samenwerking tot stand zou kunnen komen.

De samenwerking die binnen dit instituut gebundeld moet worden bestaat niet alleen uit samenwerking tussen nationale staten, maar moet ook ruimte bieden voor ISP’s, bedrijfsleven, consumentenorganisaties en direct marketeers. De aanpak moet bestaan uit een combinatie van mogelijke spambestrijdingsmaatregelen: wet- en regelgeving (en daadwerkelijke handhaving daarvan), zelfregulering (waar mogelijk), technische filters en voorlichting.

Wat het bedrijsleven betreft zou een grote speler zoals Microsoft het voortouw kunnen nemen om de grote spambestrijders om de tafel te zetten en samenwerking te faciliteren. Er kan door Microsoft op dit gebied echter niets geforceerd worden. Hiervoor zou echter eveneens supranationale samenwerking op overheidsniveau een oplossing kunnen bieden.

In beide gevallen zou een (institutionele) facilitator de verschillende typen onzekerheden kunnen beheersen. Wat betreft onzekerheid over inhoud kan de facilitator door de actoren (letterlijk) bij elkaar te brengen en ze gezamenlijk om de tafel te zetten op deze manier helpen om een gemeenschappelijk referentiekader te scheppen waarbinnen de actoren samen naar een oplossing op zoek gaan. Onzekerheid over instituties kan de facilitator reduceren door regels op te stellen voor het overlegproces, al dan niet in samenwerking met de betrokken actoren. Om een gevoel van gezamenlijke verantwoordelijkheid op te roepen is het aan te raden om voor het laatste te opteren. En om aan strategische onzekerheden tegemoet te komen kan de facilitator, voortbouwend op de eerdere suggesties, als mediator dienen indien het vertrouwen bij actoren niet voldoende aanwezig is, of als dit beschadigd is.

7.4 Afsluitende overwegingen

Aan het eind van hoofdstuk zes vroeg ik mij af of spambestrijding niet slechts symptoombestrijding is. Daar zou de vraag aan toegevoegd kunnen worden of het niet ongeacht het antwoord op die vraag een illusie is dat de overheid überhaupt bij machte zou zijn om sturing te geven aan de steeds complexer wordende samenleving. In deze scriptie ben ik er van uitgegaan dat dit wel degelijk mogelijk is. De maakbaarheid van de samenleving is beperkt, maar een poging om enige ordening aan te brengen in de chaos is wel het minste dat je kunt doen.

En in de praktijk zie je bij spam dat er een langzame ontwikkeling naar meer samenwerking is, dus ik sta niet alleen in mijn opvatting dat er mogelijkheden zijn om problemen zoals spam op te lossen of op zijn minst zo ver mogelijk in te dammen. Mijn scriptie biedt slechts de handvatten om die samenwerking waar mogelijk te versnellen.

Verder viel het mij bij het nalezen van het WRR-rapport ‘Staat zonder land’ op dat de correcte voorspellingen die de WRR in 1998 deed over de gevolgen van ICT-ontwikkelingen op de maatschappij zo slecht omgezet zijn in een beleidsvisie bij de Nederlandse overheid. Die reageert in de praktijk slechts op de problemen van de dag. Een poging om die een slag voor te zijn wordt nauwelijks ondernomen. In plaats daarvan zet de Nederlandse overheid slechts de richtlijnen die vanuit de Europese Unie worden geformuleerd met betrekking tot spambestrijding om naar nationale wet- en regelgeving.

En dat terwijl juist de politiek het soort aanbevelingen dat de WRR doet moet gebruiken om het beleid van richting te doen veranderen, opdat ze zelf nog een sturende factor blijft in de maatschappij in plaats van dat ze gestuurd wordt door allerlei processen waar ze zelf nauwelijks meer enige invloed op uit kan oefenen. Het toekomstbeeld is toch dat bij besluitvorming functionaliteit in plaats van territoir centraal zal staan, dus politiek, klamp u niet langer vast aan fysieke grenzen. Uiteindelijk bestaan die alleen in uw gedachten. Grenzen zijn slechts een *virtual reality*.

Kirsten Verdel
Moulins-Engilbert, 4 november 2004

Nawoord

De tien dagen Frankrijk waarin ik mijn scriptie afgeschreven heb zijn op allerlei punten vreemd geweest. Op de derde dag liep ik buiten in korte mouwen (eind oktober!) terwijl het slechts 11 graden Celcius was. Door de zon leek het namelijk wel 24 graden te zijn. Maar dit was nog niet half zo'n vreemde gewaarwording als de ontwikkelingen in de wereld die zich in deze ene week ineens opstapelden: de moord op Van Gogh, de dood van De Kneet op diezelfde dag, de herverkiezing van Bush, het overlijden van Arafat... Naarmate er meer gebeurde nam de concentratie op mijn scriptie af, maar dankzij Jan en Barbara kon ik mij er elke keer weer toe zetten om verder te schrijven.

Als ik dit schrijf ben ik de puntjes op de i aan het zetten. Ik moet de samenvatting nog schrijven, de noten doorlopen, de literatuurlijst in orde maken, spellingscontrole uitvoeren, de bijlagen toevoegen en de afkortingenlijst nog eens checken. En Jan is nog bezig om de laatste hoofdstukken door te lezen, dat wat hem niet duidelijk is moet ik ook nog even wijzigen in de tekst. Maar zolang de inhoud een beetje op orde is, ben ik nu dus klaar.

En toch voelt het nog niet alsof ik klaar ben. Dat heeft natuurlijk alles te maken met het feit dat ik eind dit jaar eerst nog voor 4,5 maand naar Canada vertrek om daar nog wat vakken te doen die ik aan mijn lijst toe wil voegen. Paradoxaal genoeg heb ik óók het idee dat ik juist al maanden klaar ben. Begin maart, toen ik aan mijn scriptie begon, wist ik al wat de conclusie zou zijn. En die conclusie staat nu nog steeds. Al in september schreef ik een artikel in het Financieel Dagblad met dezelfde strekking en ik had toen al een beetje het gevoel dat ik klaar was. [115]

[115] Zie bijlage D

En zo wil dit hoofdstuk maar niet echt afgesloten worden. Maar ik moet verder en ik ga verder. Nog even die puntjes op de i waar ik het net over had, nog even genieten van Frankrijk, nog even discussiëren met Jan en Barbara, nog even naar Canada, nog even afstuderen...

Kirsten Verdel
Moulins-Engilbert, 5 november 2004

Literatuurlijst

ANP, *'Nieuwe Amerikaanse antispamwet werkt niet'*, Metro (10-02-2004)

Baggott, Rob en Harrison, Larry (1986) '*The Politics of Self-Regulation: The Case of Advertising Control*,' Policy and Politics 14 , blz. 143–160

Bakkeren, Hanno '*Spamoorlog*', Management Team (12 maart 2004), nummer 4, blz. 42-44

Bekkers, V.J.J.M. (1998) Grenzeloze overheid, *over informatisering en grensveranderingen in het openbaar bestuur*, Samsom, Alphen aan de Rijn, blz. 195-196

Benson, J.K. (1978) The Interorganizational Network as a Political Economy, in: L. Karpik (ed.), *Organization and Environment: Theory, Issues and Reality,* London: Sage Publications, blz. 229-235

Bruijn, J.A. de & E.F. ten Heuvelhof (1995) *Netwerkmanagement-strategieën, instrumenten en normen,* Lemma Uitgeverij, Utrecht, blz 9

Bruijn, J.A. de, E.F. ten Heuvelhof en R.J. in't Veld (2002) *Procesmanagement*, Academic Service, Schoonhoven, (2e herziene druk)

Derksen, W.J. (2001) *Institutionele Politiek. Over de vernieuwing van de sociale zekerheid en de gezondheidszorg* (oratie) Rotterdam: Erasmus Universiteit

Frissen, P.H.A. (1996) *De virtuele staat: politiek, bestuur, technologie: een postmodern verhaa,* Academic Service, Schoonhoven, blz. 116

Frissen, P.H.A. (1993) *Zelfregulering en besturingsconcepties*, in: Ph. Eijlander, P.C. Gilhuis en J.A.F. Peters (red.), Overheid en zelfregulering, Zwolle: W.E.J. Tjeenk Willink, blz. 176

Glasbergen, P., (1989) Milieubeleid: *theorie en praktijk*, VUGA, 's-Gravenhage, blz. 233

Hawley, Anne E. (1997) 'Taking Spam Out of Your Cyberspace Diet', *Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, University of Missouri at Kansas City Law Review 66, blz. 381–423

Held, David (ed.) (2000) *A globalizing world? Culture, economics, politics.* Routledge, New York, blz. 22-24

Internet loopt vol met 'spam', de Volkskrant (05-04-2004)
Kickert, W.J.M., H.J. Aquina & F.A. Korsten (eds.) (1985), *Planning binnen de perken; Nieuwe zienswijzen op planning in het openbaar bestuur*. Kerckebosch bv, Zeist, blz. 138

Kickert, W.J.M. and J.F.M. Koppenjan (1997), Public Management and Network Management: An Overview, in: W.J.M. Kickert, E.H. Klijn and J.F.M. Koppenjan (eds.), *Managing Complex Networks, Strategies for the Public Sector,* London: Sage Publications, blz. 43

Kingdon, John W. (1995) Alternative Specification. In J.W. Kingdon, *Agenda, Alternatives, and Public Policies*, New York, N.Y.: Harper Collins College Publishers, blz. 82

Klijn, E.H. & J.F.M. Koppenjan (1997), '*Beleidsnetwerken als theoretische benadering: een tussenbalans*', in: Beleidswetenschap, nr. 2. blz. 148-150

Klijn, E.H. & J.F.M. Koppenjan, in voorbereiding (2004). "*Managing uncertainties in networks*", blz. 1, 4, 7, 36, 45, 48, 84, 161, 204, 228

Laan, Marc (2004) *Spam zal blijven*, Het Parool (22-04-2004)

Nas, Sjoera (2002) *Praktisch bekeken: spamfilters,* JAVI (december 2002), nummer 3

OECD, Directorate for science, technology and industry, Committee for information, computer and communications policy, *Background paper for the OECD workshop on spam*, 22 januari 2004 (verkrijgbaar via http://www.oecd.org/sti/spam)

Prins, J.E.J. (1999) *Over de grenzen van electronic commerce en recht*, In Mureau, D (Ed.), Fiscale aspecten van internet, UvT, Tilburg, blz. 46-62

Rogers, D.L. & Whetten, D.A.(eds) (1982), *Interorganizational Coordination: theory, research and implementation*. Ames Iowa State University Press, Iowa, blz. 54-72

Sorkin, David E. (2001) *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. Law Review 325-2001, blz. 325-384

TACD (2004), *Consumer Attitudes Regarding Unsolicited Commercial Email (spam)*, TACD Secretariat, 24 Highbury Crescent, London N5 1RX, UK

Teisman, G.R. (1997) *Sturen via Creatieve Concurrentie, Een innovatie-planologisch perspectief op ruimtelijke investeringsprojecten*, Oratie Katholieke Universiteit Nijmegen, 7 november 1997.

Wildavsky, Aaron en Ellen Tenenbaum (1981) *The Politics of Mistrust, Estimating American oil and Gas Resources*, Sage Publications Inc., Beverly Hills, California

WRR (1998) Staat zonder land. *Een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie.* Rapporten aan de regering, 54. Sdu Uitgevers, Den Haag, blz. 8-9, 44, 53-55

Wetgeving

Instituut voor Informatierecht (2004) *Regulating spam, Directive 2002/58 and beyond*, Amsterdam, Universiteit van Amsterdam, blz. 12, 36 en 63

Richtlijn 95/46/EC van het Europees Parlement en de Raad van 24 oktober 1995 aangaande de bescherming van persoonsgegevens en het vrije verkeer van die gegevens voor individuen

Richtlijn 97/7/EC van het Europees Parlement en de Raad van 20 mei 1997 aangaande de bescherming van consumenten met het oog op overeenkomsten op afstand OJ L 144.

Richtlijn 97/66/EC van het Europees Parlement en de Raad van 15 december 1997 aangaande het verwerken van persoonsgegevens en de berscherming van privacy in de telecommunicatiesector OJ 1998 L24/1-8.

Richtlijn 2000/31/EC van het Europees Parlement en de Raad van 8 juni 2000 aangaande bepaalde juridische aspecten van informatiediensten, met name elektronische handel, in de interne markt OJ L178/1.

Richtlijn 2002/58/EC van het Europees Parlement en de Raad van 12 juli 2002 aangaande de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, OJ L201

United States Congress (2003) *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, gezien op 30 oktober 2004, op
http://www.spamlaws.com/federal/108s877.html

Voorzieningenrechter Rechtbank Amsterdam (2004) *LJN: AO3649, KG 04/65 SR*, gezien op 12 mei 2004, op
http://www.rechtspraak.nl/uitspraak/show_detail.asp?ui_id=56942

Internet

AFP (2004) *Nothing but Spam, Spam, Spam*, gezien 12 maart 2004, op
http://smh.com.au/articles/2004/03/08/1078594272339.html

Bits of Freedom (2004) *Code e-mail reclame bevat verrassing*, gezien op 23 juni 2004, op
http://www.bof.nl/nieuwsbrief/nieuwsbrief_2004_13.html

Brightmail (2004) *Spam statistics May 2004*, gezien op 2 juni 2004, op
http://www.brightmail.com/spamstats.html

Brightmail (2004) *Spam statistics June 2004*, gezien op 4 juli 2004, op
http://www.brightmail.com/spamstats.html

Crocker, Dave (2004) *E-mail history*, gezien op 15 maart 2004, op
http://livinginternet.com/e/ei.htm

Elburg, Anton van (2003) *Handhaving nieuwe spam-wet volstrekt onduidelijk*, gezien op 12 juni 2004, op
http://www.emerce.nl/archives/nieuws/Media_Marketing/15207.html

Interview NSS (2002) *Ongevraagde e-mailreclame meest irritante reclame*, gezien 26 februari 2004, op
http://www.interview-nss.com/index.cfm?p=3036&l=3&act1=3&act2=0

McWilliams, Brian (2004) *Swollen Orders Show Spam's Allure*, gezien 1 maart 2004, op
http://www.wired.com/news/business/0,1367,59907,00.html

Messagelabs (2004) *Spam statistics 2003-2004*, gezien op 2 juni 2004, op
http://www.messagelabs.com/viruseye/threats/default.asp?tabIt=spam&spamduration=Last+12+months&spamgraphtype=bar&spamdata=volume

Monkeys (2003) *Spam defined*, gezien op 5 mei 2004, op
http://www.monkeys.com/spam-defined

NLIP (2004*) Reactie NLIP op Wetsvoorstel cybercrime*, gezien op 16 maart 2004, op
http://www.nlip.nl/nl/info/main/pers040310.html

Nucleus Research (2003) *Spam: The Silent ROI Killer*, gezien op 15 juni 2004, op
http://www.nucleusresearch.com/research/d59.pdf

OECD (2004) *About OECD*, gezien op 1 november 2004, op
http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html

OECD (2005) *Work on Spam,* gezien op 24 maart 2005, op
http://www.oecd.org/department/0,2688,en_2649_22555297_1_1_1_1_1,00.html

Planet Internet (2004) *Mondiale coalitie tegen spam gevraagd*, gezien op 2 februari 2004, op http://www.planet.nl/planet/show/id=118880/contentid=442381/sc=633591

Reclame Code Commissie (2004) *Code voor e-mailreclame opgenomen in Nederlandse Reclame Code*, gezien op 14 juni 2004, op http://www.reclamecode.nl/rccmenu/persbericht.asp?persberichtID=93

Reijnders, Maarten (2002) *AbFab mag abonnees XS4ALL niet spammen*, gezien op 14 maart 2004, op http://www.webwereld.nl/nieuws/10511.phtml

Reijnders, Maarten (2004) *Brinkhorst: voorlichting over zombienetwerken*, gezien op 28 oktober 2004, op http://www.webwereld.nl/nieuws/19876.phtml

Reuters (2002) *Arizona shuts down firm in alleged penis pill scam*, gezien 26 februari 2004 op http://www.siliconvalley.com/mld/siliconvalley/news/3361653.htm

Smallzine (2004) *Aantal spam e-mails neemt explosief toe,* gezien op 5 april 2004, op http://www.smallzine.nl/load.html?artikel.php?ID=7833&ACTION=

Spampoison (2004) *Verweer u tegen spammers*, gezien op 14 september 2004, op http://dutch-5041111489.spampoison.com

Spamvrij (2004) *Frequently Asked Questions*, gezien 4 april 2004, op
http://www.spamvrij.nl/werkwijze/faq-watisspam.php

TACD (2004) *'The Future Of WIPO' - Summary Report*, gezien op 1 november 2004, op
http://www.tacd.org/docs/?id=261

Templeton, Bad (2004) *E-stamps*, gezien op 13 mei 2004, op
http://www.templetons.com/brad/spam/estamps.html

Templeton, Brad (2003) *Reaction to the DEC Spam of 1978*, gezien 26 februari 2004, op
http://www.templetons.com/brad/spamreact.html

Templeton, Brad (2004) *The first spam e-mail*, gezien op 5 maart 2004, op
http://www.templetons.com/brad/spamreact.html

Templeton, Brad (2003) *The origins of spam*, gezien op 9 maart 2004, op
http://www.templetons.com/brad/spamterm.html

Tschabitscher, Heinz (2004) *What You Need to Know About Bayesian Spam Filtering*, gezien op 29 oktober 2004, op
http://email.about.com/cs/bayesianfilters/a/bayesian_filter.htm

UN (2004) *Basic facts about the United Nations: International Law*, gezien op 1 november 2004, op http://www.un.org/aboutun/basicfacts/inetlaw.htm

Verhagen, Laurens (2004) *Antispammaatregelen VS nog weinig effectief*, gezien op 30 oktober 2004, op http://www.webwereld.nl/nieuws/18587.phtml

Verhagen, Laurens (2004) *Schadepost spam: 874 dollar per werknemer*, gezien op 15 maart 2004, op http://www.webwereld.nl/nieuws/15527.phtml

WIPO (2004) *About WIPO*, gezien op 1 november 2004, op http://www.wipo.int/about-wipo/en

WIPO (2005) *Intellectual Property Issues in Advertising*, gezien op 12 maart 2005, op http://www.wipo.int/sme/en/documents/ip_advertising.htm#P241_42604

XS4ALL Helpdesk (2001) *Wat is spam?*, gezien op 22 mei 2004, op http://www.xs4all.nl/helpdesk/mail/spam

XS4ALL (2002) *DNS Blocklists*, gezien op 29 oktober 2004, op http://www.xs4all.nl/helpdesk/mail/spam/blocklists.html

Bijlage A - ‘Darkmailer’ E-mail

Van: Tiffany Edmonds
Datum: Dinsdag 2 maart 2004
Aan: trinidad@xs4all.nl
Onderwerp: Spam for you!

Hello!!

Dark Mailer Version 1.36 by Janell!! (www.darksoft.biz)
Anonymous Bulk Email Software

Dark Mailer is a super fast bulk email software that sends out at speeds greater than 1,000,000 emails per hour* on a dedicated mailing server. Dark Mailer has the capability to use Proxies and Relays and also to send directly.

Some of the features include:
Anonymous Mailing using Proxies
Message Randomization to bypass Spam Filters
Speeds over 850-950K emails per hour on Turbo Mode
Up to 1000 Threads

Unlimited Email List Size (up to 100 Million per file)
HTML and Plain Text Emails
Tag Macros to personalize and randomize emails
Custom Headers ..... more on
http://www.darksoft.biz

Julio Ferguson.
www.darksoft.biz

Janell!!
synergy grimaldi architectural bamberger bitch chafe burundi bedbug malcolm alert droop cavitate british billiard shelter enunciate bedridden centipede legume brillouin levity cooky eidetic specific dwindle metier insecure dean archbishop ducat endothelial gully coffin timbre demark wingspan ded=
uce descent=20

----19081110074155361898--

Bijlage B - E-mail van de OPTA

Van: Secretariaat Eindgebruikersmarkt
Datum: Maandag 24 mei 2004
Aan: locuta@xs4all.nl
Onderwerp: SPAM

Geachte heer, mevrouw

In antwoord op uw e-mail over spam, kan ik u het volgende meedelen.

OPTA krijgt onder de nieuwe Telecommunicatiewet de bevoegdheid om handhavend op te treden tegen verzenders van spam. OPTA krijgt deze bevoegdheid alleen voor zover het gaat om spam die wordt verzonden aan natuurlijke personen. Spam verzonden aan bedrijven valt hier dus niet onder. Een Nederlandse wet geldt alleen binnen Nederland. OPTA zal dus ook alleen tegen Nederlandse
verzenders van spam kunnen optreden. Met ingang van de inwerkingtreding per 19 mei 2004 van de nieuwe Telecommunicatiewet (Tw) kunnen particuliere eindgebruikers terecht op een OPTA-website voor het indienen van klachten tegen overtreders van het spamverbod (artikel 11.7 Tw).

Met schriftelijke vragen, telefonische vragen of vragen via e-mail kunt u niet bij OPTA terecht. Hiervoor kunt u contact opnemen met de Postbus 51 informatielijn (0800-8051). Het postadres is: Postbus 20002
2500 EA Den Haag.

U kunt ook een bezoekje brengen aan www.surfopsafe.nl. Dit is een website van het Ministerie van Economische Zaken over het veilig gebruik van internet.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Front office, OPTA

Bijlage C - “cd’s for sale’ E-mail

Email Marketing !

We offer you e-mail addresses databases(or called " email lists , email leads ,bulk email lists) for advertisement mailing; we sell databases also carry out mailing and hosting for the advertising (email broadcasting campaign) projects.

Products
World Email Lists . Their validity and originality are verified.

Country or area total emails and price

America 175 Million Email Address $220 US
Europe 156 Million Email Address $250 US
Asia 168 Million Email Address $150 US
China(PRC) 80 Million Email Address $200 US
HongKong 3.25 Million Email Address $200 US
TaiWan 2.25 Million Email Address $200 US
Japan 27 Million Email Address $200 US

Australia 6 Million Email Address $150 US
Canda 10 Million Email Address $150 US
Russia 38 Million Email Address $120 US
England 3.2 Million Email Address $200 US
German 20 Million Email Address $200 US
France 38 Million Email Address $150 US
India 12 Million Email Address $120 US
CENTRAL & SOUTH AMERICAN AREA 40 Million Email Address $220 US
MIDDLE EAST & AFRICA 45 million Email Address $220 US
SOUTH EAST AREA 32 million Email Address $220 US

other Country or Area
ÿFFFFA1ÿFFFFADÿFFFFA1ÿFFFFADÿFFFFA1ÿFFFFADÿFFFFA1ÿFFFFADÿFFFFA1ÿFFFFADÿFFFFA
1ÿFFFFAD
order email : hosting@watches.netpublications.net or
targetemailrequest@btamail.net.cn

Bijlage D - Ongevraagde e-mail bestrijden kan met een gezamenlijke aanpak (FD 7-9-‘04)

(Het Financieele Dagblad, dinsdag 7 september 2004)

Ongevraagde e-mail bestrijden is mogelijk met een gezamenlijke aanpak

Op de voorpagina van Het Financieele Dagblad van maandag 30 augustus staat onder de kop 'Nederland verdient aan mail-aanvallen' een artikel over spam en de rol van Nederlandse spammers. Dit naar aanleiding van cijfers die het ministerie van Economische Zaken naar buiten bracht. Het artikel levert een aantal vraagtekens bij mij op.

Zo zegt Economische Zaken dat 1,2 procent van de ongevraagde mail uit Nederland afkomstig is en daarmee de wereldwijde toptien haalt. Nog geen week geleden verscheen er een onderzoek van virusbestrijder Sophos waarin juist werd gesteld dat het aantal spam -e-mails vanuit Nederland flinkgedaald is. Met 0,67 procent vallen we inmiddels in het niet bij de Verenigde Staten (42,5 procent) en Zuid-Korea (15 procent). Maar zelfs als we nog wel in die wereldwijde toptien zouden staan, is de vraag wat we aan die informatie hebben om spam te bestrijden. Wat wel noodzakelijk is, want spam kost de Nederlandse economie handenvol geld. Van internetprovider Xs4all weet ik, omdat ik er werk,

8 DINSDAG 7 SEPTEMBER 2004

Ongevraagde e-mail bestrijden kan met een gezamenlijke aanpak

Spam is geen Nederlands probleem

7

dat er jaarlijks 368.000 euro uitgegeven wordt aan extra servers en personeel om spam te bestrijden.

Tom Kok van het platform voor direct marketing DDMA (Dutch Dialogue Marketing Association) noemt een paar oplossingen voor het spamprobleem, zoals elektronische postzegels inzetten als spambestrijdingsmiddel. Maar veel spam wordt tegenwoordig via virussen verspreid. De postzegel wordt dan dus niet door de spammer betaald, maar door besmette pc-gebruikers. De spammers zullen er niets van merken in hun portemonnee. Maar ondertussen zou wel het hele idee van internet als gratis, openbaar, wereldwijd communicatiemedium te gronde gaan. Betalen voor e-mail is niet de oplossing, maar zou juist voor een nieuw probleem zorgen.

Een tweede stelling van Kok is dat de meest effectieve methode van spambestrijding een boete is. Na die uitspraak meldt het artikel doodleuk dat er in Nederland nog geen enkele boete is uitgedeeld. Dat is niet zo vreemd, want spammers zijn door slimme technische trucs nauwelijks te traceren. Ze gebruiken daarvoor virussen, die niet alleen spam versturen maar ook nog eens mailadressen op besmette pc's plunderen om die ook te spammen. Verder vervalsen ze afzenderadressen, ze zetten verminkte woorden in e-mails om filters te ontlopen die afgericht zijn op woorden als 'viagra' of 'sex' en ze maken misbruik van slecht geconfigureerde mailservers van nietsvermoedende internetgebruikers om daarover hun spam te versturen.

De Nederlandse wetgeving (voortkomend uit een Europese richtlijn) voorziet alleen in de aanpak van Nederlandse spammers. De meeste spam komt, zoals we net zagen, juist van over de grens. De onlangs door toezichthouder Opta ingestelde website spamklacht.nl waar 'particuliere eindgebruikers' kunnenklagen over spam uit alleen Nederland heeft dan ook niet veel meer dan een symbolische functie. De door Kok voorgestelde boetes zijn dus, als ze er al komen, slechts een druppel op een gloeiende plaat.

Maar we zijn nu dan ook bij het echte probleem aangeland: spam is niet aan grenzen gebonden. De Wetenschappelijke Raad voor het Regeringsbeleid schreef in 1998 al dat veel activiteiten dankzij ict wereldwijd kunnen worden ontplooid, onafhankelijk van de

geografische locatie. De afnemende binding met grondgebied die hier het gevolg van is, heeft volgens de WRR 'onvermijdelijke gevolgen voor het handelingsvermogen van de nationale staat'. Wet- en regelgeving zijn immers onlosmakelijk aan territoir gebonden. Maar de benodigde grensoverschrijdende samenwerking om spam te bestrijden wil maar niet van de grond komen. De meningsverschillen over alleen al de definitie van spam zijn nog te groot: is alleen commerciële e-mail spam , of ook mail met een wervende politieke of charitatieve boodschap?

Maar hoe dan wel? Uiteindelijk is spam alleen te bestrijden door een gezamenlijke aanpak van consumenten, internetproviders, overheden en consumentenorganisaties. Die aanpak zal moeten bestaan uit betere wet- en regelgeving, zelfregulering waar mogelijk, goede technische spamfilters,'user awareness' (het bewustzijn bij de ontvanger van de e-mail dat het niet verstandig is om op de e-mail in te gaan) en betere voorlichting aan de burgers. Wat dat laatste betreft heeft ook de Nederlandse overheid nog een lange weg te gaan. Minister Brinkhorst dacht zich er met een heroïsche oneliner vanaf te kunnen maken. 'Don't ask what your country can do for you, but what you can do for your country', zo citeerde hij onlangs John F. Kennedy. Met andere woorden: 'zoek het zelf maar uit'.

Maar een Nee/Nee-sticker op de digitale brievenbus plakken, werkt helaas niet.

KIRSTEN VERDEL

Kirsten Verdel is studente bestuurskunde en werkzaam bij internetprovider XS4ALL.