Stratix

The size and business case of spam in the Netherlands

A report to DGTP, Ministry of Economic Affairs

By Stratix Consulting

Schiphol, December 2004

Stratix

Table of Contents

Stratix

Executive Summary

Unsolicited electronic mail sent in bulk volume promoting commercial, political or charitable ends - *spam* - is responsible for the majority of today's total e-mail traffic. The daily flood of spam, in most cases originating from other countries, has grown into a considerable problem for Internet users. This report provides an overview of the rising problem of spam received in the Netherlands. It describes the nature, the size and the cost spam reception and countermeasures impose on various groups in society. The report calculates the costs of a campaign by senders of legitimate (opt-in) bulk e-mail and compare that to the costs senders of spam encounter. On this basis we show the mechanisms behind the business case for spam to determine potential intervention points for government policy.

Nature, size, cost and the business case of spam

In the past decade an arms race developed between a group of fringe entrepreneurs, that send out unsolicited bulk e-mail to (in some cases) millions of e-mail addresses, harvested from various internet sources, and ISPs and corporate owners of mail servers. This autumn the daily volume of spam received in the 10 million Dutch mailboxes has reached 145 million messages per day, close to two thirds arrives in consumer inboxes. This volume constitutes 75% of the daily incoming mail. More than 99% of all incoming spam is of foreign origin and appears to be part of globally distributed undirected spamruns.

The number of Dutch spamruns directed at Dutch users in the Dutch language has fallen below 2 per day since the new anti-spam articles of the Telecommunications Act came into force in May 2004. OPTA[1], responsible for enforcing the new articles, has received 3586 admissible complaints. 90% of the complaints concern spam, 8% concern unsolicited text messages (SMS) and 2% regard junk faxes and automated telephone calls. Hardly any complaint has yet been filed about spam from a high-profile firm or brand on the Dutch market, nor has there been any complaint with regard to a political or charity promotion. The Dutch sources turn out to be a cluster of marginal entrepreneurs, who seem to trade address lists and spam tools frequently. Interviewed experts estimate that volumes per Dutch spamrun amount to several tens of thousands.

Spam causes several major problems. One of them is its negative effect on social trust in the Internet as a reliable platform for information exchange and transactions. It therefore hampers the growth and development of the Internet in society. These generic

[1] Onafhankelijke Post en Telecommunicatie Autoriteit, the Dutch telecommunications regulator.

social consequences of the floods of spam are important but its total costs are difficult to quantify.
As an example: the daily flood of spam could cause a large loss in productivity and requires additional download time for dial-up end-users accumulating to € 1,688 billion per year. In view of the various countermeasures taken, such as spam tagging & filtering, new legislation, monitoring, investigation and enforcement, a realistic figure for the cost of spam in the Netherlands is € 116 million (See Table).

Table: *The cost of spam without and with countermeasures taken*

	Without any anti-spam actions	**With countermeasures**
Loss of social trust & annoyance	p.m.	p.m
Productivity loss	€ 1,667 million	€ 83.3 million
Extra Dial up cost	€ 21 million	€ 10.0 million
Spam-filtering:		
• Client based programs		ca. € 2.0 million
• Server based incl. staff		€ 20.0 million
Bandwidth	€ 9,000	€ 9,000
Defining policies		€ 0.2 million
Monitoring & Enforcement		€ 0.5 million
Cost of spam in NL	€ 1,688 million	€ 116.0 million

Desk research revealed that most client based spam filter programs are freely distributed in limited functionality (trial-) versions. Consumer and small business end users comprise the main market. Full functional versions sell at a typical price of US$30. Based on sparse vendor reports on installed base we estimate annual spend in the Netherlands on these programs at € 2 million.
It is more efficient to perform spam filtering on mail servers and this is the locus of most counter efforts today. In our field interviews we found most ISPs and large corporate users experience a typical cost of € 1 per mailbox per year for operating anti-spam systems. Small & Medium-size Enterprises that deploy their own mail servers encounter an annual cost of approx. € 5 per mailbox, due to lower economies of scale. Even with adequate filtering not every user will activate the highest protection levels, to avoid important messages to be mistaken for spam.

Spam does not consume excessive bandwidth. Messages are typically not more than a few kB. The largest cost for ISPs and mail server owners lies therefore in the staff needed to administer the servers. Over the past three years these technical efforts needed to handle, counter and clean up after spam have doubled the annual cost per mailbox for operating an e-mail service.

People sending spam today need to buy or create five inputs: a spam program, access to a mail server or *proxies*[2], an e-mail address list, network access for sending messages to the proxies, a bulletproof website to collect potential customer replies. A contract with an on-line payment system to conclude transactions is a potential sixth input, but this part of the transaction can also be handled off-line, depending on the nature of the goods or services sold. The majority of virus-explosions on the Internet during the last two years are attributed to efforts of spam ventures in creating *proxies* for their business. One could therefore also add access to skilled virus creators as an input. Most inputs can be purchased per month for a few hundreds of US$ and used for spam runs sending out several hundreds of thousands messages per hour. Depending on quality of *proxy lists* and *addresses* the prices can go up to several thousands of US$.

The popular unsolicited bulk e-mail program, *Send-Safe,* also sells for a reduced price of US$ 199 but is bundled with a number of credits and a limited list of proxies. Send-Safe lists a price of US$ 100 for 1 million credits with a staggering schedule up to US$ 3,000 for 300 million credits. Based on these observed prices we estimate that the aggregate of hard core spammers responsible for the large majority of 145 million daily incoming e-mails in the Netherlands are spending ca. US$ 15 thousand per day to reach potential Dutch customers. This is equivalent to US$ 0.0001 per message. From this we conclude that senders of spam spend in the range of € 4 million per year to reach potential Dutch clients.

Legitimate senders of bulk e-mail incur campaign costs that rapidly rise above € 0.20 per e-mail, depending on campaign size and the specificity of the e-mail address rented (where prices vary from € 0.04 to € 0.40 per address). The DDMA[3] estimates that the total expenditure of their sector on e-mail marketing in the Netherlands is € 100 to € 125 million per year.

Direct marketers claim success rates for e-mail marketing that are far higher than for conventional postal mail. The customer acquisition costs for a postal mail campaign is about € 80 per win. For e-mail it falls to a few Euros due to higher response rates.. If spammers are able to convert one customer out of every million messages they send, they bear a customer acquisition cost of US$ 100. If they convert one customer per 10,000 outgoing e-mails their acquisition cost falls to US$ 1 per customer.

It is clear that the profitability for the business case of senders of spam depends critically on their customer acquisition costs and reach. The barrier of entry for a hard core spamrun is still relatively low. It costs up to € 1000 to start with a relatively high-quality list of addresses. Intervention can be directed the factors that determine the cost

[2] In most cases these are hacked or virus-infected computers that have been transformed into hidden Spam gateways without the owner's consent.
[3] Dutch Dialogue Marketing Association

in the business case: the inputs required by spammers, as well as their reach to recipients. Interventions can be aimed at deterring entry or raising the cost of submitting a high volume of unsolicited e-mail to end-users.

We have found the following potential intervention points to damage the business case of spammers:

- Purchasing a spam program
- Control over (a list of) proxies or access to mail relays or servers
- Buying or harvesting e-mail addresses
- Network access
- Bulletproof webhosting
- The financial payment system
- The cost of reaching out to recipients
- 'Willingness to buy' of a recipient
- Skills to release Zombie-PC viruses

Establishing a toolkit for countermeasures
In the final chapters, we describe the number of technological, behavioural, legal and economic countermeasures already taken by various actors. We list and categorise those measures per group of actors - End-users, Internet Industry, Legitimate Senders and the Government - to assess visible gaps in coverage, and provide a toolkit. Several recent proposals and initiatives for new approaches and interventions are added to the systemic toolkit. The report finishes with addressing the question of allocation of responsibilities and authority for the new elements in the toolkit, listing those not yet taken up or brought to their full extent, and recommending policy initiatives.

An overview of current countermeasures drawn from the interviews and found by desk research reveals that most can be characterised as technological and behavioural (social / organisational). The new legislation, which came into force in May 2004, added a set of legal instruments and introduced involvement of the Government. Most of the still few economic countermeasures are still indirect. The cost for sending spam is raised through legal deterrence with administrative fines and limiting, throttling or tarpitting traffic.

The list of current countermeasures derived from several new proposals from our interviews, and of the gaps we found by categorising both in the framework for the toolkit, was compared to the potential intervention points that damage the business case for senders of spam.

A number of countermeasures are oriented towards denying spammers network access; some are oriented towards limiting their access to proxies, mail relays and mail servers. Also, behavioural efforts to educate end-users not to respond to spam and hand out their e-mail address with care tend to make address-acquisition, -verifying and updating less easy and therefore more costly. Most technological measures and the prohibitions and clauses in legislation are oriented towards limiting the number of recipients reached by spam and requiring authentication of the senders.

We found that many proposals still attempt to raise the cost of reaching out to end-users by non-economic means. One proposal attempts to address the economic problem. The external cost imposed on the recipient is not internalised in the system and is not signalled back to the sender in the form of a fee. This route, called *e-stamp*, has not yet been tried nor thoroughly researched.

Few countermeasures address potential intervention points in the business case, such as the commercial availability of spam programs, the way e-mail addresses are acquired, bulletproof webhosting and the link to financial payment systems required by spammers to complete the transaction.

We therefore recommend that a number of measures are taken by the various actors and stakeholders.

1. End-users should know how to behave with regard to spam and take preventive measures (the Government, Internet industry, Consumer-organisations and employers can assist with an information campaign).
2. The Internet industry should implement measures on all levels (hardware, software and network) against spam distributed through proxies (zombie PCs), like authenticating mail servers, and support collective anti-spam initiatives.
3. Legitimate senders should show the origin of the address (list?) used to send the e-mail, to facilitate de-listing from the original list.
4. The Internet industry ISPs filter and screen outbound mail on bulk e-mail characteristics, applying bulk limits, PPO (= Prior Permission Only)
5. The government and OPTA should explain the extent of the Telecommunications Act's anti-spam articles[4] to the public, and in particular to the (small) business community, in far more detail.
6. The government should convene representatives of all actors to establish a serious study on the viability of voluntary and multi-party (self-regulation-) approaches to implement sender pays mechanisms.
7. A similar initiative should be taken at the EU-level, with at least FEDMA, Euro-ISPA, BEUC, the ERG and EDPS represented.
8. The government should focus Dutch efforts on outbound spam, and the use of (viruses to create) open proxies and engage in international co-ordination for inbound spam.
9. The government should study present and future legal options to intervene at points in the business case not yet explored in current countermeasures, such as the sale of spam programs, the trade in access time to proxies, the link to a financial payment system, bulletproof webhosting and the manner in which address lists are acquired.

[4] In particular which persons and small businesses are covered due to the category *natural persons* of Article 11.8 requires better explanation.

We propose to strengthen the authority of law enforcement agencies for investigating and tracing hard core spammers, as many operate on the shady side of business. Private investigation and tracing by ISPs is not recommendable except when asked for by Law Enforcement. The government may improve the means for ISPs to report a major attack on their systems, by opening a road to report to a national High Tech Crime Centre instead of the local bureau. The law enforcement agencies could also co-ordinate the establishment of *honeyproxies* with ISPs, whose log files then can be used in the prosecution of Zombie PC users.

Stratix Consulting

Schiphol,
December 2004

Stratix

1 Introduction

Unsolicited electronic mail sent in bulk volume promoting commercial, political or charitable ends - *spam* - is responsible for the majority of today's total e-mail traffic. Estimations on the amount of unsolicited bulk e-mail range from 50% (European commission) to over 80% (July 2004, Dutch ISPs) of the incoming e-mail. Hotmail, the leading web-based e-mail service operated by Microsoft, reports spam blocking of 2.7 billion out of 3 billion incoming messages, a day ratio of 90%.

Spam has become a very large part of the daily electronic message inflow. Many corporations, Internet Service Providers (ISPs) and end-users have implemented tools to tag, discard, filter and block unsolicited bulk e-mail. Volunteers have started initiatives to collect abuse reports and enlist e-mail servers that function as a source of spam. However, these technical countermeasures have not proven sufficient yet to reduce the amount of spam, as senders of unsolicited bulk e-mail have introduced ways to circumvent blocks and filters. Substantial pressure has been exerted on Governments to legislate this issue. In addition, the borderless nature of the Internet has created an international co-ordination problem for aligning legislation and enforcement.

In the Netherlands, the new revised Telecommunications Act came into force in May 2004, implementing recent European Directives. In articles 11.6 and 11.7 provisions are written to outlaw the sending of unsolicited e-mail promoting commercial, idealistic and charitable ends to end-users and instituting administrative penalties and enforcement on misbehaviour by OPTA, the Dutch Telecommunications Regulatory Enforcement Authority. As an iterative process, this can be considered a first step in the public legislative domain. Many other developed countries have now taken similar steps.

However, as the problem of spam keeps changing and evolving it is necessary to improve legislation and be aware of all instruments available to remedy the growing spam problem. This can only be done with a good overview of the nature, size and costs of the problem, the economic and social costs for end-users and of countermeasures taken in the network, the effects on end-users as well as knowledge of the business case for senders of spam. This report explores these issues and lists countermeasures taken by various actors, whether of a technological, legal, social-organisational or economic nature. The goal is to fill in a toolkit of countermeasures in an organised approach, and to raise awareness of potential gaps. Potential intervention points will be indicated by a comparison of the business case for spam and the toolkit.

1.1 Report outline

In chapter 2 of this report we provide a short overview of the mounting problem of spam and the variation in definitions of the problem, both in the literature and by our interviewees. We analyse the nature and the size of spam in the Netherlands in chapter 3. From our interview and fact-checking findings, we estimate the costs and the distribution over the various actors involved in chapter 4. This provides the context for exploring the mechanisms behind the business case for spam we present in chapter 5. Chapter 6 describes the countermeasures already taken and categorises them. The systemic toolkit is presented in chapter 7, which we also use to explore holes and gaps and to characterise several recent proposals and initiatives, which were presented to us. We conclude with chapter 8, where we address the issue of allocation of responsibilities and tasks in the developed toolkit and provide recommendations for policy initiatives.

1.2 Issues addressed in this report and research responsibility

The goal of this report is to analyse the situation in the Netherlands. It is therefore constrained to the Dutch situation, though it is obvious that parts of the problem are of a global nature. We have limited the study to unsolicited electronic e-mail. The study's focus does mean we will only briefly touch issues like *mobile spam*, *viruses* via e-mail, *autodiallers, spyware* and other *malware,* and the fraud part of *identity theft* solicited via e-mail *(phishing)* when relevant.

The research has been performed by a desk study of studies and descriptive material and several Internet sources, an internal expert review by the team, and a series of interviews and fact checking sessions conducted in person and by telephone. We interviewed ISPs who serve different segments of the Dutch Internet market. We also interviewed the IT staff of a multinational enterprise serving 50,000 Dutch employees, about 1% of the Dutch business users[5]. We also have interviewed representatives of *spamvrij.nl* and the Dutch Dialogue Marketing Association (DDMA) to investigate the contrasts in the value chain for both legitimate bulk e-mail and spam, to detect differences. We held fact-checking interviews with other organisations and gained insight in several new initiatives and countermeasures currently under development or in pilot.

In this report, a quantitative estimate is made of the nature, size and cost of spam and its effects in the Netherlands. This assessment is performed with data of several interviewed companies that are quite diverse in the market segments they serve; together they represent several percent of the total number of Dutch e-mail usage. In our assessment our quantitative extrapolations to the entire Dutch market are quite reasonable. They have been reviewed by experts and compared with assessments of ISP veterans and ISP representatives.

[5] The total workforce using PCs in the Netherlands is approx. 5 million

2 The growing problem of unsolicited bulk e-mail

Unsolicited bulk e-mail, frequently called 'spam', is a mounting problem. Its roots lie in the specific background and culture from which the Internet originated. A number of properties of the original networked mail user groups, which differ substantially from today's Internet user community, have influenced the mail-protocol design. This does not mean that the phenomenon of spam and the sometimes rather strong reactions of recipients are a recent problem. A look at the development of the problem illustrates the interrelated nature of the mail protocol and technology design, the user groups and their habits and how they responded. A short overview of the historic development, and the technical arms race that has developed over the years between senders of spam and recipients (ISPs and organisations), is provided in the first section. In the second section we elaborate on the different definitions interviewees used of what they consider spam. This illustrates the divergence between stakeholders in assessing and defining the problem.

2.1 History

2.1.1 The historic roots of unsolicited e-mail

The first unsolicited e-mails appeared on mailing lists already in the seventies. On the ARPAnet, the predecessor of the Internet, it was a commercial message by a Digital Equipment Computer representative, promoting their newest model. This led to irritation and responses resulting in electronic disputes named ‘Flame Wars’. The still rather closed e-mail user groups reacted to this by introducing the rules of behaviour known as *Netiquette*. Organisations/Systems administrators were required to sign an AUP: Acceptable Use Policy. In larger organisations, the system administrator confronted the person sending unwanted messages. This pragmatic solution, social pressure, did not last when the Internet became available to everyone in the nineties. Some people saw a new business opportunity in Usenet, mailing lists and e-mail to reach a large public for their messages, which allowed them to avoid being subjected to social pressure.

The first commercial e-mail globally depicted as spam dates from 13 April 1994. The message was sent to Usenet newsgroups and selected mailing lists by a law firm, ‘Cantor and Siegel’. The firm had in mind to recruit potential US immigrants as customers by inviting to assist them for joining the Green Card lottery. Their acts and the consecutive course of this case reveal the core of the spam problem and its business case: many senders operate in the shady areas of their professional and social associations. Cantor and Siegel had already been suspended by professional law associations and expelled from the Bar.

2.1.2 E-mail and other types of unsolicited communications

Spam on the Internet is not a new social phenomenon; other communication technologies suffer from unsolicited messages too. Call centres employ many outbound telemarketers, various organisations attempt to send commercials as text messages (SMS), and junk faxes containing commercial messages are responsible for almost all incoming faxes these days. In the Netherlands many postal mailboxes carry stickers rejecting commercial flyers. In all cases the sender of unsolicited commercial information must overstep a considerable cost barrier per electronic or paper message.

The prime difference between unsolicited bulk e-mail on the Internet and conventional technologies is in the division of costs incurred by parties in the value chain of spam on the Internet. The costs of designing a campaign, producing, sending, routing & forwarding, receiving, storing and reading e-mail fall on different organisations. Proven social self-regulatory concepts like public defamation (naming & shaming), peer pressure and exclusion of 'sinners' from industry associations do not function properly, and globally applicable laws and punishments are lacking. This has started a technology race.

2.1.3 The spam arms race

In the unsolicited bulk e-mail technology race both (corporate) users deploying their own e-mail servers and ISPs have taken several countermeasures. These countermeasures vary from a change of configuration parameters, by which third parties can abuse the mail-server as an open mail forwarding system, to the introduction of spam tagging software, spam filters and protection software to detect unwanted incoming messages. Many of these countermeasures are taken on the receiving side for the purpose of reducing the nuisance and wasted time of private persons and employees, and to reduce their vulnerability for viruses sent by e-mail.

To clamp down on clients that originate spam on their network most ISPs have revised their Acceptable Use Policies, general terms of trade and commercial contracts. They also opened abuse desks and co-operated in establishing spam detection and blocking lists and/or supplying information. Most ISPs adhere to a set of use policies of what is considered good practice in the industry, however some ISPs seemed to have evaded this and allowed large-scale spam operations to continue from their network. In such cases a most severe sanction was applied to the ISP: *the Internet Death Penalty,* which means that all major Tier 1 backbones decided to refuse further routing of traffic from and to this ISP. As this sanction also hurt the ISP's regular clients this has proved highly effective in the Western World. However ISPs encounter difficulties in approaching peers on some other continents

Some of the spam-senders terminated their activities when ISPs started to clamp down on sources of unsolicited bulk e-mail that originated from their own network, enforcing terms of trade, contracts and acceptable use policies, but others looked for new means to access networks.

2.1.4 Sending spam through open relaying

The first alternative means was found in *mail server open relaying*. Relaying is the ability of mail systems to forward to any other system in the world. Originally a feature of the e-mail protocols for making the e-mail service more robust, open relaying is now considered a flaw and an e-mail system allowing open relaying is regarded as badly configured. Spam senders started to scan the Internet for *open relay servers*, and lists of IP-addresses of open relay servers were on the market. To reach the open relays several programmers developed and started selling specific *Bulk Mailing Software*, as it is not easy to submit e-mail to tens of thousands of users with an ordinary mail client program.

In response, many ISPs and corporate end-users reconfigured their e-mail servers. However, initially this required quite some education on the part of corporate end-users. A second measure was taken on a global scale by volunteering system administrators (often linked to ISPs). They established various block lists with mail-servers and known open relays reported by users.

2.1.5 Sending spam through hacked and virus-infected machines

After efforts to educate the system administrator community and to reduce the amount of open relays gained traction, the number of access opportunities decreased considerably. Several spammers developed programs that create stealth open relay servers by hacking insufficiently secured PCs of unsuspecting users. As system security has improved for most professionally operated servers, spammers have shifted their approach from hacking to releasing and distributing computer viruses (by e-mail, or through downloading from webpages) that install the relaying server program utilising viruses that capture end-users' PCs.

The virus-infected and hacked machines are accessible through 'back doors' and operate as *'proxy gateways'* for conveyance of the spam. These are commonly known as *zombie PCs*, as non-expert broadband users are frequently unaware their machine has been captured to serve as an open mail relay. Russia-based software vendor SendSafe[6] provides its bulk e-mail programs with lists with IP addresses of zombie PCs and port scan tools to find them. The countermeasure to recognise and combat these forwarding techniques has only recently been developed by some ISPs.

[6] http://www.send-safe.com/

2.1.6 Recipients improved spam tagging and filtering

In the last few years spam tagging and blocking software has improved from primarily utilising blocking lists as a source of information, to less or more intelligent heuristic analysis of mail headers, and advanced statistical (Bayesian) techniques to analyse the text in the incoming mail on frequent word usage and sentences.

Most messages that are sent through these captured relaying servers contain (commercial) fringe offerings or illegal products and services, such as lifestyle-drugs, prescribed drug that can be obtained without a prescription (anabolic steroids, Viagra, Prozac etc.), adult entertainment, shark loans and shady money laundering proposals (the so-called Nigerian 419). They can often be recognised by statistical techniques, due to a combination of use of words, colour and capitals and the fact that the bodies of a large number of incoming messages are the same. The simple heuristic filters however fail to hold back most spam as senders have developed methods to circumvent and mislead them.

Today the most advanced heuristic filters use Bayesian statistics. These can be trained with typical spam. They are self-learning on the pattern of received mail to discern *false positives*[7] and *false negatives*[8] from *true* spam recognition to a very high degree. Faced with this advanced information technology at a serious scale, spam sources started to add a large variety of words from dictionaries, *Bayes-Busters,* to make their e-mail look more like ordinary texts and circumvent and confuse these filters.

2.1.7 Shifting the arms race from the private to the public legal domain

Vendors of spam software programs[9] are now offering potential spam senders various testing possibilities to assess their message's ability to pass certain filters. In addition, they even provide tools to avoid so-called honeypots, the spam traps installed by users to detect sources or proxies used for spam.

Consequently, the arms race continues and claims have increasingly been laid at the doorstep of Governments to enact legislation. Many experts[10] contend that spam is a

---

7 A false positive, also called false alarm, exists when a test reports incorrectly that it has found a signal where none exists in reality. Detection algorithms of all kinds have the tendency to create such false alarms. (Source: Wikipedia)

8 A false negative, also called a miss, exists when a test reports incorrectly that a signal was not detected when, in fact, it was present. For example, radar not detecting an enemy airplane when an enemy airplane was present within the radar scanned area. (Source: Wikipedia)

9 Currently: *Dark Mailer* and *Send-Safe* are the most popular.

10 Including Dave Crocker, the editor of the original RfC 822 e-mail standard

social phenomenon and the probability to counter it completely with technology is close to zero.

2.2 Definitions of spam differ

It is not difficult to describe the more offending types of messages that people consider spam, but it is difficult for many, including legislators, to define spam. This becomes clear when we compare the new articles written in the Dutch Telecommunications Act, existing definitions in the literature, and definitions given by our interviewees. Their answers are listed in the next section. The views of one interviewee on categorising the submitters of unsolicited bulk e-mail illustrate the problem in the consecutive section. In 0 we have listed Articles 11.7 and 11.8 of the Telecommunications Act and the Explanatory Statement for the recent changes (in Dutch).

2.2.1 Definitions of spam

Our interviewees gave the following limitative, but rather divergent definitions of spam and (unsolicited) bulk e-mail.

- Unsolicited bulk e-mail. It is difficult to verify that permission has or has not been given. Therefore *unsolicited* is a difficult concept. *Unsolicited* should rather be replaced by *undirected*. Bulk could be appended with the words *with ease* or *without effort*.
- An electronic message is spam if:
  a. the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND
  b. the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND
  c. the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

Internal mail is never spam. In an operational sense, spam detection software determines what spam is.

- From the ISP perspective: e-mail sent to non-existent e-mail addresses.
  From the customer perspective: received e-mail the customer does not actually want. (For this reason the customer is allowed to self-configure what he considers spam)
- Unsolicited bulk e-mail is sending e-mail to illegally acquired addresses.
  Unsolicited is a very clear concept. *Undesired* is a strongly subjective concept.
- E-mail directed to multiple persons with almost similar contents that promote a commercial, charitable or political message.

The subtle difference of the latter definition with the actual text of the Dutch Telecommunications Act lies in *multiple persons*. This interviewee opposes the current legitimacy of unsolicited bulk e-mail to corporate employees due to Article 11.8 of the

Dutch Telecommunications Act. This article has defined an opt-in regime for natural persons (mainly consumers) and entails an opt-out regime for most employees. The problem is that this definition is not as clear-cut as it seems[11]. A substantial number of consumers use their corporate account or a sports club account as their main e-mail channel. This issue was discussed in Parliament, but amendments to article 11.8 failed to win a majority.

Most senders of unsolicited bulk e-mail cannot discern between private and corporate domain e-mail accounts. Since 2003 second level domain names under the *.nl* top level have also been sold to consumers[12] in the Netherlands. One of the interviewed ISPs observed that some senders of spam seem to explain the new Act as a license to send unsolicited commercial mail to accounts with names such as info@domain.nl, sales@domain.nl or office@domain.nl, avoiding account names that look like surnames.

2.2.2 Categorisation of groups of spammers

One of the interviewees, the Spamvrij Foundation, has attempted to categorise the senders of spam. They have arrived at three main categories:

1. Hard core spammers
2. Main sleaze spammers
3. Opportunists

Hard core spammers are people that break the law in every respect. Main sleaze is the name for a group of direct marketing agencies that are testing the boundaries of the Act or are operating just outside of it. This is a complex group. Opportunists are companies who send spam but do not realise what they are doing. Spamvrij tries to educate these opportunists once they are reported.

While the hard core category is primarily driving the technology race, as they are utilising the latest tricks and opportunities to (re)gain access for mass mailing (today these are zombie PCs and mass mailers from East Asian cities), it is the main sleaze group that makes the legal discussions on spam so complex.

Spamvrij lists several of the members of EMMA-NL (Electronic Mail Marketing Association - Netherlands) in their main sleaze spammers category. EMMA, a sector association of mass e-mail service agencies and Application Service Providers, claims

[11] Article 11.8 restricts the applicability of the opt-in regime to natural persons. Consequently, one could also interpret the Act to mean that sending unsolicited commercial e-mail to Dutch enterprises that lack the status of legal entity is not allowed. Such companies constitute the majority of small businesses that are registered as firms, independents, free lance contractors, professionals, etc.

[12] Until 2002 the .nl-domain registry required a Chamber of Commerce number for the registration of a second level domain under *.nl*, effectively restricting it to (not-for-profit) corporations.

to operate on the legal side of the sector. They differ from hard core spammers in that they operate their own mailing systems from their own domains. They are not engaging in activities such as hijacking PCs and hit-and-run tactics to gain access to the network.

2.2.3 Size of the mailing is not a good discriminator

The root of the conflict in the legal definitions of spam lies in a difference of opinion between Spamvrij and main sleaze spammers on the legality of their activities. This also touches on the various opt-in and opt-out regimes the Dutch Telecommunications Act provides for between mail to consumers and corporate employees.

Several interviewees have indicated that they use the size of the bulk mailing as a means of discerning categories. This fails as a good test. We found that the EMMA members mainly serve smaller businesses, since large corporations have now set up their own systems or are outsourcing to e-mail service agencies. They frequently send legitimate mailings to former customers or (business) contacts from addresses they have acquired. In some cases ass mailings from certain Dutch organisations with a large social reach (e.g. millions of users of their (non-profit) services) amount to hundreds of thousands of e-mails per mailing. In most cases these mailings are larger than the typical extent of spam reported. However it is highly probable that (a combination of) other traffic data can serve to identify a mailing as spamming.

3 Nature and size of the spam problem

In this chapter we will elaborate on the nature and the size of the problem of spam in the Netherlands. It concludes with a quantitative assessment of the amount and origins of spam received in the Netherlands.

3.1 Technologies and actors involved in a spam transaction

To analyse the nature of spam it is necessary to sketch what tools are needed and whom is (un) consciously co-operating with a spammer to reach out to the end user and establish a successful transaction. Figure 3-1 shows that on an abstract level the acts to reach out, transact with the recipient and fulfil the order does not differ betweeen a legitimate sender of bulk e-mail.

The real differences between a legitimate sender of bulk e-mail and a sender of spam reside in the nature of the tools. They need a bulk e-mail program that has dedicated spam features, an acquired address list or a tool to harvest e-mail addresses from the Internet, access to an e-mail conveyor via a list of proxies, open relays or a contract with a rogue hoster willing to install a mail-server. In that last case one speaks about a hit-and-run mail server or *"bulletproof"* server, often operated until the rogue hoster receives a complaint from his upstream ISP.

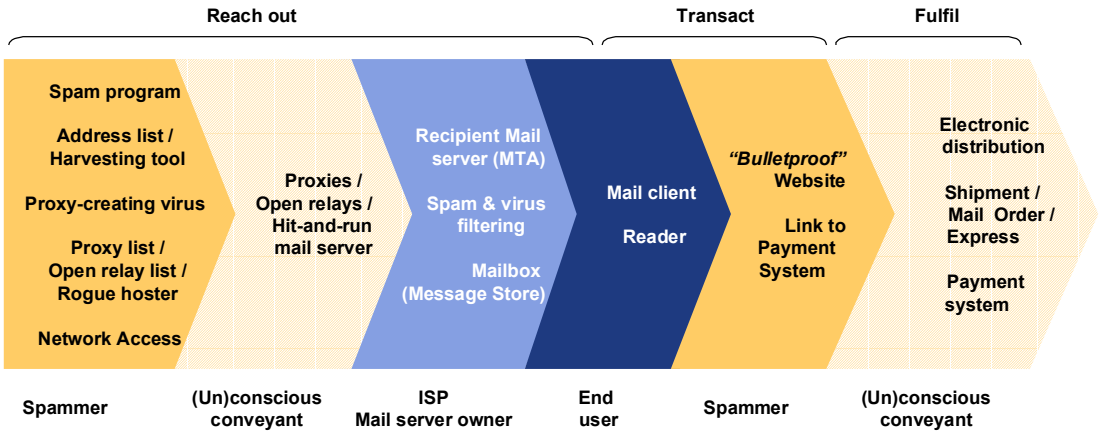


Figure 3-1 *The chain of technologies and systems involved in a spam transaction*

Unconscious persons and organisations, whose systems are not well configured or due to a virus changed into a proxy, can become a conveyor of the spam message. When a spam message arrives at the mail servers of an ISP or an end user, it can be led through spam-filtering functions before ending in the message store. End users can fetch the message with a mail-client or gain knowledge of its content via a (web-based) reader and decide whether to respond to the offer.

Most attention is given to the start of spam and the route it requires to reach the end user. But to complete the transaction with a recipient, willing to buy a service or a good from a sender of spam, the spammer also need to establish a "*Bulletproof" website*. A link to an (electronic) payment system is not essential but often rather desirable too, due to the occasional nature of the typical spam transaction. The fulfilment step contains a second group of conveyors. They are often regular companies who may not be well aware that the transaction that caused their business stemmed from spam.

When we discuss questions about the nature, size and cost of spam, we are mainly concerned with the left-hand side of Figure 3-1. The efforts and cost to reach out to end users and the negative external effects due to the large flood of unsolicited mail is made in that part of the chain. The right hand side must however be kept in mind, as it is needed to complete the business case for a sender of spam. In the next sections we will explore the size and problem due to spam from the viewpoint of the recipient to the source.

3.2 Issues faced by recipients

Not all Internet users receive large amounts of unsolicited bulk e-mail. The problem seems to be more or less constrained to a small group, consisting of people who distributed their e-mail address to a larger audience in the past. These are either long-term Internet users who used their e-mail address in public (archived) Internet areas when spam was practically non-existent and they were not yet aware of the problem. Other users who receive large amounts of spam are people who provided their e-mail address on a number of websites or gave it to a large number of organisations. However, protection of users' e-mail addresses by using them carefully is becoming difficult because many viruses harvest personal e-mail address books and add the addresses to spam lists. Following this development even confidential e-mail addresses can be subject to spamming.

Recently *dictionary attacks*[13] were reported as a new method to find e-mail addresses. The interviews revealed that these attacks seem to be directed more to large mail-domains, with tens of thousands to millions of users. This method to reach out to mailboxes still seems to be directed primarily to selected consumer (mass) ISPs. The multinational enterprise we interviewed had the impression that they were not yet under such attacks, due to the facts that they used a divisional structure in the domain part of the e-mail address[14].

[13] Spam senders attempting to second guess e-mail account names by putting in random account names and variations from a frequently used names list (dictionary)

[14] E.g. username@division.firmname.nl

From our set of interviews and fact checking efforts, we received the following data about spam volumes and the size of mail operations.

Table 3-1 *spam for selected segments of mail system operators*

Market segment	# Customers/ Employees	# Mailboxes	Incoming mail (3Q2004)	spam (%)
ISP: Consumers-Broadband	100,000+		1.6 million per day	54%
Activated spam filters		~ 45,000		35%
ISP: SME	~ 5,000	~ 60,000	400 thousand per day	80 - 99%
ISP: SME			100 thousand per day	90%
Corporate: MNE	~ 50,000	~ 50,000	6-8 million per month	30%
Corporate: SME	~ 25	~ 35	1000 - 2000 per day	65%

ISPs and corporate users find higher percentages of incoming spam in the weekend due to the fact that businesses tend to communicate far less in that period. Figure 3-2, published by specialist ISP Pine Digital Security, shows the incoming spam as a percentage of the total incoming mail as 80% on average.

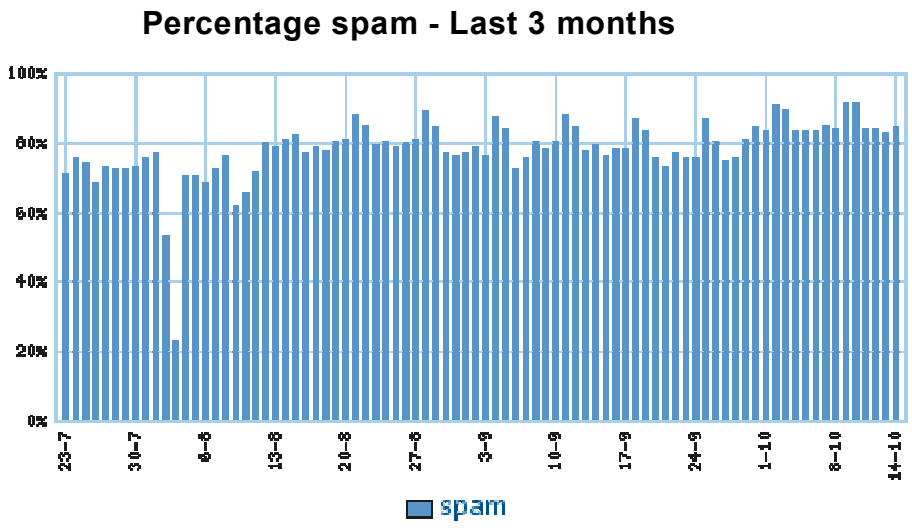


Figure 3-2 *Incoming spam percentage for Pine Digital security, an SME oriented specialist*[15]

Pine's statistics still show a daily increase in spam. This is in contrast with the views expressed in the interviews by other ISPs and spam organisations. They saw spam stabilising since June 2004. The corporate user we interviewed had experienced a growth of spam from approximately 7% to 30% in less than a year.
One of the more striking features in all interviews was the relatively limited interest in activation of spam filters by end-users. A minority of the consumer broadband ISPs subscribers has activated the free web-based spam filter. Neither do all SME clients ask for helpdesk assistance and implementation. Even inside a large corporation, most

[15] http://www.pine.nl/page/67

users tend to start activating the rules to discard spam in their Outlook client only when the IT department added simple ***spam*** tags in the subject line. More elaborate e-mail headers indicating spam classifications that were used during the piloting of the spam detection techniques were overlooked.

Another important finding was that virus scanning and mechanisms to protect against them are considered far more important than spam filtering by all mail system operators. The priority for virus scanning is probably higher because a virus outbreak causes much greater damage. It is clear, however, that the problem of zombie PCs links viruses and spam

3.3 Growing processor and traffic load at the service provider

The interviewees largely agree when questioned about the network elements that are stretched by the growth in spam. All interviewees agreed that spam was and is not a bandwidth problem today. Frequently non-spam e-mails contain large file-attachments, but spam typically runs at a few kiloByte per mail. Spam puts stress on e-mail systems, on maintaining them and on (abuse) helpdesks.

However, views diverge on which part of the e-mail service is most affected. The consumer ISP states that installing the spam block and filtering of e-mail for users takes so much disk space that it pays to invest in more processing power. On the other hand the corporate user and SME oriented ISPs are primarily blocking virus-mail and consider conserving server processing power more important than diminishing the use of disk space. Important incoming mails are valued highly in a business environment.

Another difference is the matter of *dictionary attacks*. The consumer ISP has to defend against this with strong countermeasures and it is the cause of the 54% of spam being blocked at the ISP-level. It is the percentage of traffic directed at non-existent usernames in their domain. With mail blocks using large username directories, they are rejected at the edge of the e-mail systems (not straining and polluting mail-servers in the process). Consumers that activate spam filters remove another 35% of the 46% of e-mail that enters the mail systems.

Dictionary attacks however seem to be more a problem for organisations in which spam senders are expecting hundreds of thousands of subscribers than for smaller companies or corporations that have employees' e-mail systems organised in divisional domains. The corporate user we interviewed has not yet observed a dictionary attack on their systems. They only tag incoming spam at the entrance of their network and forward e-mail to servers deeper inside the company, therefore a dictionary attack would have been observed immediately inside the e-mail system.

ISPs have stated that with a growing number of consumers activating spam filters they have to invest in more servers. For large ISPs these ongoing costs are quite visible. When discussing total costs of anti-spam efforts we found however, that updating spam filters and systems to detect the latest varieties[16] and staffing the help desk functions are the most visible effects of the rising spam burden. Several ISPs and corporations outsource the effort to specialist firms to keep track of the continuously changing landscape in spam filtering rules or to provide rapid response virus filtering. According to one of the interviewees roughly 20 firms operate around the globe which have specialised in constructing advanced spam and virus filtering platforms and provide mail cleansing services in various flavours. UK-based Message Labs is the most visible of these firms, due to its advertising campaign. The interviewed parties that do not construct platforms themselves had hired different firms.

Like ISPs, large corporations tend to install dedicated servers to detect spam. The effort to maintain them is considerable to keep pace with spam senders' latest circumventions. Smaller companies often integrate the functions of spam filtering and virus filtering with a software utility or other third party software add-on into their mail server systems. This is not all that different, as these tools need frequent upgrades as well.

3.4 Technology bulk e-mail utilised and required by senders

It is possible to send e-mail to large numbers of recipients with conventional e-mail systems. This requires considerable effort, as most e-mail programs are not designed for this. This has been recognised at an early stage by mailing list operators, so a number of specialist mailing list programs like Mailman, Listserv and Majordomo have been developed especially for this purpose. A central problem for large mailing lists has been the handling of the address database. This comprises subscription to and removal from the list and the automated insertion of the e-mail addresses into the outgoing mail. A large number of organisations deploy mailing list software to send newsletters and information to their contacts. The original mailing list software is often used by not-for-profit organisations. It is frequently installed by ISPs as a supplementary service for their client base. Yahoo! provides a well-known web-based mailing list management service with their eGroups offering[17].

Mailing list software was probably too limited for the demands of corporate users, as a result of which some software developers have produced more specific bulk e-mail software to cater for the more specific market of commercial newsletters. These programs can be purchased and used for both legitimate use and spam. Vendors often

[16] One of the most difficult new spam types to detect are mails consisting of only stock market information. Such almost random information circumvents most intelligent filters. Without any source they probably attempt to influence stock market prices and speculators.

[17] http://groups.yahoo.com/

have high-profile clients, which they list on their website as an endorsement of their legitimacy.

Not every organisation has the scale or the professional IT-resources to operate this software or to develop it in-house. Service agencies have seized the opportunity to assist them with e-mail marketing. They either operate the specialised software or deploy in-house developed software and tools in an applications service provider model.

Hard core spammers deploy different software and tools, as they need to circumvent ISP's acceptable use policies. They also deploy tools to harvest e-mail addresses and to test their unsolicited e-mails against filters.

This section lists several of the technologies for sending bulk e-mail that go beyond general mailing list software, their features and some known providers.

3.4.1 Do-it-yourself technologies

People and organisations that are planning to submit a bulk e-mail can deploy a standard e-mail client and their own or their ISP's mail-server. They can insert the recipients list in the *bcc*-field[18]. A disadvantage of this method is that distribution of the e-mail stops if one address in the list is refused (bounced) by a receiving server. Moreover, it is impossible to personalise the messages. One needs a MailMerge function to perform personalisation, which is possible with some clients, but requires many manual steps, which is clumsy for larger volumes.

Consequently, many people and organisations are shifting to mailing list software or specialist bulk e-mail programs. One of the most-used programs is BulkMailer, sold for $198 by the German vendor, Kroll Software[19]. In the Netherlands e-commerce software vendor Data Becker[20] sells a comparable program *Mail to Date* for € 99 through their website, but also through the Makro, Office Center and Dixons retail channels.

Organisations that do possess sufficient in-house IT skills can develop their own system by installing and adapting open source mailing list software. A product in this category is Dada Mail[21].

[18] bcc: Blind Carbon Copy
[19] http://www.kroll-software.de/produkte/bulkmailer_en.asp
[20] http://www.databecker.nl/software/webdesign/mailtodate.html
[21] http://www.dadamail.org/

3.4.2 Several service agencies provide solutions for bulk e-mail

A number of e-mail marketing service agencies have sprung up in the Netherlands. Most of them are associated in EMMA-NL[22]. They provide web-based self-service (ASP-model) and/or (web-based) full service (outsourcing model) to send bulk e-mail. Members of EMMA-NL are listed in Table 3-2.

In our interviews Veritate Company and RapidSugar were most often mentioned as companies most active in the service agency segment. Other firms deploying the ASP model are, www.informaxion.nl, www.yourzine.nl, www.e-mark.nl, www.scope.nl. These service agencies often deploy customised programs and in-house developed software. ING subsidiary Postbank is also a member. Asked during the interviews for an indication of current legitimate bulk e-mail volumes in direct marketing, Postbank was mentioned as an organisation that mails volumes of several hundreds of thousands to their clients per mailing run.

Table 3-2 *Current members of EMMA-NL*

- 06 Software
- Besides Purple
- Composite Digitale Media
- Doors International
- e-Markethings
- Euroclix
- E-village
- HCB Media
- Hot SMS
- Interambition.com
- Measure mail
- Netdirect
- Postbank
- Qamel Intelligente e-mail campagnes
- RapidSugar
- Sellvation Marketing
- Veritate Company
- Webxpose
- Webpower

Although a recent press article mentions companies like Postbank and KLM as users of full service outsourcing of e-mail marketing, it is stated that most large corporations are now shifting the operation of bulk e-mail to their in-house IT department. The marketing department of the large corporate user interviewed for this study also sends out bulk e-mail, as well as unique messages, reporting electronic transactions performed by customers from its own facilities. E-mail is therefore a tool of growing importance for businesses.

3.4.3 Companies sell solutions to hard core spammers

Organisations submitting large volumes of unsolicited e-mail have developed specific programs that differ substantially from mailing list software and tools like Bulk Mailer. Some developers have started selling these programs to third parties, in

[22] E-mail Marketing Association Nederland, http://www.emma-nl.net/

combination with a portfolio of supplementary tools: CD-ROMs with e-mail addresses, and programs to harvest e-mail addresses from the Internet.

Besides their Mail Sender, Subscription Manager Atomic[23] sells a large set of independent utilities to harvest and verify e-mail addresses from all kinds of sources: Email Hunter, Newsgroup Explorer, Address Verifier, Whois Explorer, CD Email Extractor, Mailbox Password Cracker and IE Contacts Spy (e-mail addresses on webpages). The combined package of all utilities costs US$ 433.50. Atomic also provides a bulk SMS Messenger program, charging users per message.

ContentSmartz[24] is another provider of mail address harvesting and bulk mail sender software with a highly professional-looking website. According to them their mail sending software has the technical ability to submit up to 50,000 outgoing mails per hour. A combined package of various address harvesting and mail management and sending software can be purchased for US$199.

Atomic and ContentSmartz mail sender programs still require the use of a stand-alone server or the ability to submit through the outgoing corporate or ISP mail server. As such the main difference between this vendor and Kroll Softwares BulkMailer is the large set of e-mail address harvesting tools. However, it is possible to use this type of software if one knows how to turn a badly-configured mail-server into an open relay.

The reality today is that the hard core groups that are held responsible for 90% of global spam are deploying different tools today. They have converted to *stealth proxies*, often installed on zombie PCs, infected by viruses. One vendor of these programs is MTI Software (4577 Gunn Highway #161 Tampa, FL 33624, USA). They offer their Desktop Server program with an add-on for sending through proxies. In their advertising they gloss over the specific nature

> One of the problems in the past when using a mail server was that you needed port 25 available, which many ISP (but not all) block these days. Also your Internet IP address can show in the headers of the message you send, allowing some advanced users to send in a complaint to your ISP. Those days are over with the new Proxy add-on for Desktop Server!
>
> Here is how it works: Some systems on the Internet are left publicly available as a proxy server so people can browse the web, chat, or even send email anonymously. Many concerned with their privacy use proxy servers to maintain their anonymity. You can do the same with Desktop Server when sending your bulk email.
> **http://www.desktopserverpro.com/desktopserver.htm**

[23] http://www.massmailsoftware.com/buy /
[24] http://www.contentsmartz.com/index410.htm

of the proxies that are used, suggesting they are voluntarily made available as proxy servers for anonymous submission of e-mail.

Interviewees indicated that DarkMailer and SendSafe bulk e-mail software is today's most popular tool for hard core spammers. Send-safe software is sold as a stand-alone version for US$199 and as a site license for $799. They seem to go a step further than MTI software, by selling supplementary tools like Proxy Scanner, Honeypot Hunter and a testing tool to circumvent advanced filtering programs. Send-Safe operates with time-limited licenses of 30, 60 and 90 days and sells at different prices for different credit volumes. The program discounts credits by the number of successful e-mail deliveries. Send-Safe is capable of sending up to a few hundreds of thousands of mails per hour[25], depending on the number of proxies used in parallel, the amount of outbound bandwidth available to the sender of the mail run and the number of e-mails per connection with a mail server.

When starting a session Send-Safe users receive a list of current open proxies from Send-Safe. They can add their own proxies by hacking PCs and installing the necessary software either by distributing a virus that installs the proxy or by hiding the proxy in a program with some executable that is installed from a website. It is also possible to distribute open proxy programs by including them in spyware or adware programs, or hiding them in installers of popular fringe programs (such as various peer-2-peer programs, executables with jokes etc.). Finally they can compile their own list of open proxies by scanning (part of) the Internet. Therefore there is no direct link between someone using the open proxies and the origins of a virus that installs them.

The origin of the Send-Safe program is unclear. The domain name is registered by a Russian citizen[26]: Ibragimov Ruslan, 12 Krasnokazarmennaya, 111250 Moscow, Russia, tel: +7.957235641. This suggests a Russian origin. Some limited further research on the web server's IP address reveals that the website is probably hosted on an MTI Software server in Tampa, Florida. This is the outcome of a simple traceroute on the Internet and a reverse lookup at Whois.sc, which is not always reliable.

3.4.4 Hard core spamming in the Netherlands

It is estimated that there are no more than two or three hard core spammers in the Netherlands who send out spam on a global scale. In the press and in our interviews Martijn Bevelander and Michiel Laurentius Baas are mentioned several times. Where Bevelander got substantial press coverage, Baas; a 21 year old resident of Heemskerk, has managed to hide behind his companies while his spam activities are directed to other countries. He seems to have left the country. During an interview request

[25] This can be determined and calculated from the screenshots http://www.send-safe.com/screenshots.php

[26] http://www.whois.sc/send-safe.com

Bevelander informed us that he left the scene about a year ago. He did not respond to our suggestion that this allows him to speak out freely on techniques. Interviewees mentioned that port scans for open proxies in Dutch ISP's networks have been detected that originated from Bevelander's Cyberangels domain. The Dutch telecommunications act forbids sending spam to other countries. But it confines itself to Dutch residence of the material sender, the one that has an interest in the conveyance of the content of the spam message. To what extent operating for a fee as the 'mere' facilitator by providing access to known *proxies* and *relays* for non-Dutch spammers is considered as sufficent lack of material interest in the conveyance of the content of the message must be seen.

According to spamvrij.nl, the entire top list of Dutch spammers[27] who distribute spam in Dutch use open proxies to distribute their messages. Due to the high number of broadband connections in the Netherlands, the attractiveness of the Dutch Internet for distributing viruses that establish zombie PCs is high. They do however report a decline in spamruns from Dutch organisations directed at Dutch e-mail users since the Telecommunications Act came into force in May 2004.

3.5 Quantifying the size of spam in the Netherlands

In this section we provide an estimate of the size of all incoming e-mail in the Netherlands and the amount of spam in it. A normal weekday is the best sample for a reasonable assessment of the volume. We determined the amount of incoming spam, incoming e-mail and outgoing e-mail per market segment from data provided by various interviewed parties and compared our findings with the experts we used for fact checking. SME clients are the most varied and diverse group. They vary in size from single person firms to medium sized companies of a few hundred employees with computer access.

Table 3-3 *Key figures on the daily amount of spam and ordinary e-mail in the Netherlands*

Market Segment	# in segment 3Q2004	Inbound Spam	Inbound normal	Outbound Normal
Consumer Broadband mailbox	4.5 million	11	4	3
Consumer Dial up mailbox	4.5 million	10	3	2
SME clients	600 thousand	40 - 80	10	6
MNE employees	2 million	3 - 10	6	2
Total external e-mail messages per day		~ 145 million	~ 50 million	~ 30 million

[27] Spamvrij compiles this list from Spam recipient complaints

The daily amount of 145 million spam messages per weekday constitutes approximately 75% of all incoming mail from the public Internet. In the weekend, when there is less corporate mail, spam levels can jump to levels above 90%.

Spamvrij collects statistics on Dutch spam originating from Dutch organisations and persons and directed to Dutch users. A picture of the decline of the number of spamruns after the new legislation came into force is shown in Figure 3-3.

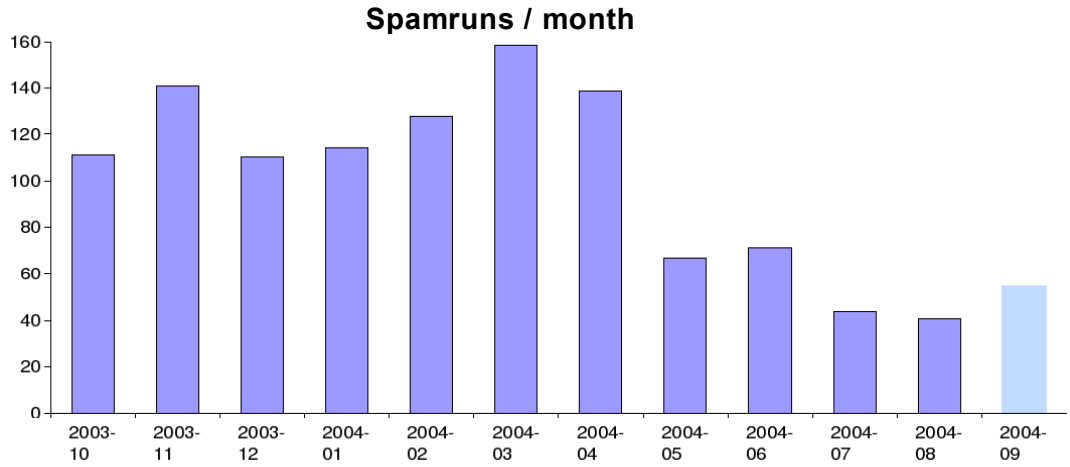


Figure 3-3 Spamruns per month from Dutch organisations to Dutch users[28]

The average size of a Dutch spamrun is several tens of thousands of e-mails. Consequently, it is dwarfed by the international inflow. However, due to its different language and specificity these e-mails pass most (English-language-based) spam filters.

It is not easy to assess the amount of spam originating from the Netherlands but terminating in mailboxes in other countries. Some of the most probable sources for statistics are the vendors of anti-spam tools and services who analyse their data to assess the IP address of the proxy or relay that sends the spam, and determine the total volume of the spam. They thus do not measure the home country of the spammer, but the location of the (in most cases unconscious) conveyor. When an anti-spam tool vendor has a sufficiently global client base, its statistics provides a reasonable impression about the amount of spam send.

When comparing several sources we conclude the participation of computers in the Netherlands in the conveyance of international oriented spam has fallen in the last 6 months. Brightmail, an anti-spam tools vendor, reported in April 2004 the Netherlands occupied a 10th slot in their global ranking of spam sources with a share of 2% of

[28] As reported to Spamvrij Foundation: http://rejo.zenger.nl/abuse/1095102631.png

message volume. The cause was probably a massive number of virus infected Zombie PC's. Brightmail has not released a country report recently, but Ciphertrust, another an anti-spam tools vendor, provides public statistics. The top list of IP-addresses involved in spam is given in figure Figure 3-4

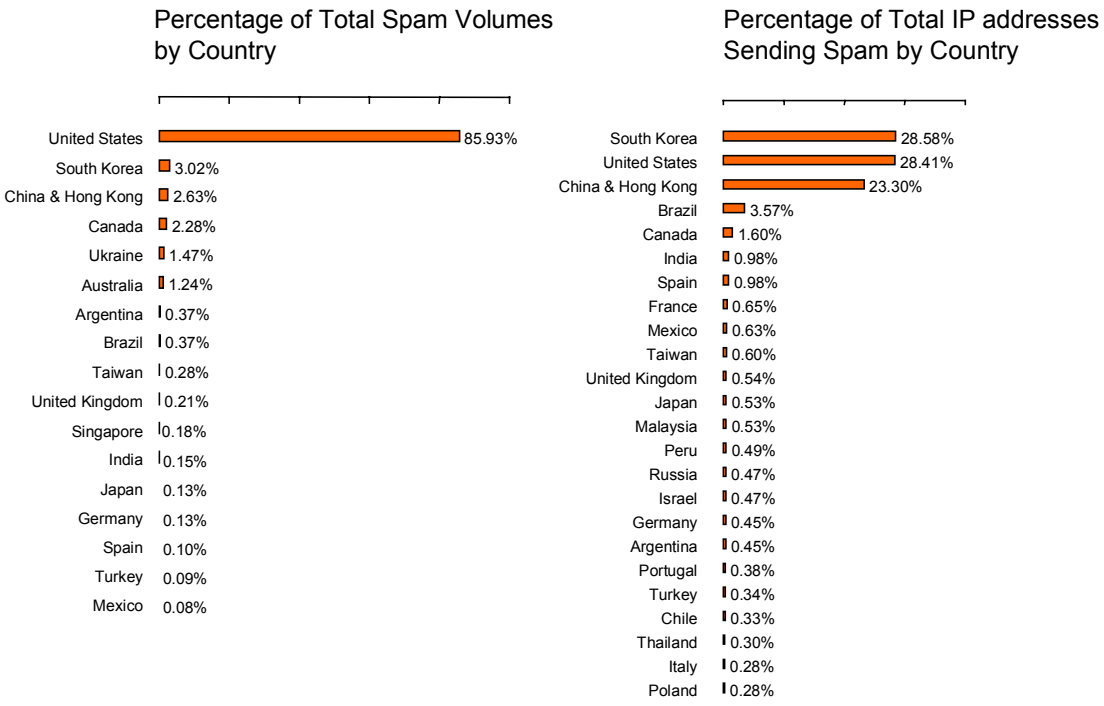


Figure 3-4 *Despite their high broadband density, the Benelux and Nordic countries are absent in CipherTrust spam statistics.*[29]

[29] http://www.ciphertrust.com/resources/statistics/spam_sources.html, CipherTrust Spam Statistics, as available in October 2004.

4 Economic and social costs of spam

In this chapter we assess the economic and social costs of spam. This is done by distinguishing four categories of costs: those incurred by the recipient / prospective reader, by the ISP and mail-server owner, and by the Government in its policy-making and enforcement efforts. The results are summarised in section 4.4. The sender of bulk e-mail also incurs cost to send spam to Dutch citizens. These are analysed in the final section and compared to the Dutch spending on e-mail marketing.

4.1 Recipient costs: productivity loss, annoyance, viruses, loss of mail, etc

4.1.1 The non-measurable cost: lost trust in the Internet as transactions channel

One of the most often mentioned but difficult to measure is *lost trust* in Internet and e-mail as a viable way to execute a transaction. This cost is imposed on any party that has a legitimate case to deploy e-mail, but shies away from selecting this channel due to the bad reputation spam has brought to it. What it does is to take away the opportunity for many parties to deploy a cost effective communications channel. The problem for this study is off course that it is practically impossible to directly measure the cost of lost trust to society. We therefore note it *pro memori*.

4.1.2 Productivity loss figures in the press are exaggerated

A slightly better measurable social cost of spam for a recipient is the time spent on recognising and deleting it. Annoyance dominates. In the corporate sphere this translates as a direct cost for loss of productivity. In the corporate sphere spam arrives in large volumes to users with a long Internet history, who used their e-mail address out in the open or provided it on websites that were set up to collect addresses for resale purposes. Dictionary attacks to harvest e-mail addresses in the Dutch corporate market have not been reported in our interviews[30]. That phenomenon seems to be more restricted to large consumer ISPs.

A frequently used statistic to assess the social cost of the time spent on spam is 10 minutes per workday[31]. Frankly, we think this is an exaggeration if applied to the total workforce. For office employees 10 minutes per workday represents approximately 2% of annual work time. Office employees that receive and read e-mail on a daily basis can be estimated as close to 50% of the Dutch economic workforce. This implies that those 10 minutes lost on spam per day for the average office worker cost the Dutch society 1% of its Gross Domestic Product in unproductive work time, i.e., € 4.5 billion per year.

[30] One corporate user and business ISPs with thousands of clients
[31] http://www.computeractive.co.uk/news/1158623

The multinational enterprise we interviewed has provided us with an internal calculation made in the summer of 2003 for its international division that operates under a *.com* domain name. The influx of spam at that time was 20% of all incoming mail. They used a figure of 10 seconds of time lost per incoming unsolicited commercial e-mail, which seems more reasonable than 10 minutes per day.

The firm we interviewed states that a number of employees added a discard rule in their e-mail reader only after the firm started adding the simple tag ****spam**** in the subject line of messages determined to be spam. If they had not facilitated their 50,000 Dutch employee workforce in this way they would have had to discard about 24 million incoming spam-messages manually. Given 10 seconds time to delete and an average employers' cost of € 50 per hour they arrived at 66.7 thousand lost working hours, constituting a loss in productivity worth € 3.3 million. A spam filter with 95% true positives and 0% false positives, a cautious spam threshold, reduces this loss in productivity to € 167 thousand per year.

In Table 3-3 we saw that in the Netherlands the total amount of incoming spam per workday amounts to 48 million messages. This implies 133 thousand lost work hours per day on a national scale and 33.3 million lost work hours per year[32], a cost figure of € 6.7 million per day. With 95% true positive spam tagging and/or filtering this is reduced to € 83 million annual cost.

As was mentioned above a substantial number of corporate users still do not receive much spam, not having handed out their e-mail address often. The internal division between employees receiving much spam and those with limited spam in their inbox is highly skewed. This means that the time lost in the corporate market mainly falls on a small percentage of employees, who may start to apply automated spam filtering as soon as it is available. The rest will probably continue to delete it manually.

We think the assessment of 10 seconds for deleting a spam message is also reasonable for the time spent by consumers. Our interviews show that a skewed distribution of spam recipients is observed in the consumer market as well. The ones to suffer the highest influx of spam are those with the longest experience and the most intensive Internet users as well as those that have left their mail addresses at sites and newsgroups. But this picture is shifting. When the time spent per day sifting through their inbox increases, they turn to their ISP to activate spam filters.

4.1.3 More reasons in favour of the decision to install spam filtering

Besides productivity disruptions and IT-resource consumption (discussed in the next section) two other factors were taken into account by the firm we interviewed:

- Spam is annoying and offensive email can be upsetting

[32] We assume 250 work days per year on average, as spam increases in the weekend

- The graphic and obscene nature of many spam emails raises concerns about legal liability[33]

Both reasons also seem to be the main source of anger in many consumers. Moreover the ongoing influx of spam reduces the reputation of the Internet as a reliable channel for e-commerce and establishes a climate of distrust for consumers. This may hamper a general uptake of the Internet as a cost efficient means and (economic) growth is stemmed. Finally, despite the rapid diffusion of broadband Internet access, about half of the Dutch households and a third of the small businesses still access the Internet over dial-up lines. They incur a real cost in additional telephone charges for downloading spam. One additional minute per day due to spam results in a cost of € 0.50 to € 1 per month (at off-peak and peak rates).

Spam is not the only problem e-mail users receive in their inbox. All parties running e-mail servers interviewed by us have stated that blocking e-mail viruses is far more important than blocking spam. On average viruses attached to e-mail comprise 1% of the incoming mail flow. Several recent viruses (*worms*) raided the local e-mail address books to find forwarding addresses. They spread to people who had not frequently handed out their e-mail addresses , which produced a much larger effect during an outbreak. No major virus outbreaks have occurred over the last months and the number of incoming viruses has fallen considerably. This is a spectacular reduction that is ascribed to the arrest of a young German virus writer, who appears to be the main source of most outbreaks in early 2004.

4.2 Costs of spam filtering are rising

The cost of spam filtering rises, due to the growing number of installations either at computers of end users or in mail-servers at ISPs or corporations. The costs are not easily observed as free, but functional limited versions of spam filter programs, are often used as a first remedy by end users, while ISPs and corporations include server based filters with the e-mail service. In this section we assess these cost more in-depth.

4.2.1 Client based filter costs for end users stabilise

End users can protect themselves by installing a spam filter program, either sold as a plug-in for popular e-mail clients or as a separate program. An Internet survey of the various programs on offer revealed that nearly all vendors sell them at US$ 30[34]. This differs from about two years ago when commercial client based filters, in particular those of security software vendors, were sold at prices around hundreds of dollars. Most vendors provide a version with limited functionality or working for a short trial period (30 days) for free. It is therefore quite difficult to obtain figures on the paid

[33] A specific notice regarding this aspect was added for their US operations
[34] http://spam-filter-review.toptenreviews.com/?ttreng=1&ttrkey=mcafee+spamkiller

installed base of end user spam filtering programs and their avoidable cost, even when providers release installed base figures. The Danish vendor Spamfighter.com is one of the few who releases per country figures[35] that show their Dutch user base is above 26,000. Their global client base reaches nearly 600 thousand with 300 thousand users in Denmark.
The market for client based spam filtering software is highly contested between e-mail program vendors upgrading their programs (e.g. Microsoft, Qualcomm etc.), renowned security software vendors (McAfee Spamkiller, Norton AntiSpam etc.), and a number of independent software vendors[36].

The Netherlands is very comparable to Denmark comparing Internet usage and broad-band penetration. It is however rather likely that an indigenous vendor sells more in its home market. We therefore estimate that the number of client based spam filtering programs in the Netherlands in the range of 750 thousand. Based on this amount and assuming most users (consumers) selected the limited feature (free) versions we estimate annual spending in the Netherlands on the 'professional' client based programs in the range of *€ 2 million*.
This figure is not expected to rise as many ISPs have now engaged in the practice of bundling free anti-spam filtering in their subscription offer. This diminishes the demand for separate client based products. The inclusion of anti-spam filters in standard e-mail clients and computer security suites is shrinking the market too.

4.2.2 Service provider costs and mail server owner costs have doubled

In our personal interviews, from media statements and by checking facts with other ISPs we have assessed the annual cost of installing and operating spam tagging and filtering software. All interviewed parties have stated that spam takes up a relatively negligible percentage (2-3%) of incoming e-mail bandwidth, as most messages are (still?) small (a few kilobytes). An incoming international flow of 145 million 2 kb spam messages per day constitutes a load of 30 Mbit/s, to be purchased from Tier 1 backbone providers. At current wholesale prices of approx. € 25 per Mbit/s per month this adds up to an added aggregate bandwidth cost of € 750 per month for all Dutch ISPs.

The parties we interviewed mention only the costs they incurred to set up their spam filtering function. This comprises servers, initial development costs and annual depreciation of this effort. The operational cost of maintaining the filters (several have outsource this task to spam filtering specialists) and the cost of servicing the users such

[35] http://www.spamfighter.com/community_countries.asp
[36] In the price range of US$30 dozens of spam filtering products are offered: Spam Inspector, SpamEater, Qurb, EmailProtect, ChoiceMail One, Spam Buster, MailFrontier, SpamNet, Spam Agent, iHateSpam, SpamSubtract, MailWasher, SpamCatcher, Spamfighter etc.

as help desks and abuse desks dominated. Typical figures for mail server operators in various segments of the Dutch market are listed in Table 4-1.

Table 4-1 *Cost of server based spam filters for selected segments of mail system operators*

Market segment	# Mailboxes	Annual cost
ISP: Consumers-Broadband	~ 150,000	€ 160,000
ISP: Consumers-SOHO	~ 400,000	€ 386,000
ISP: SME	~ 60,000	€ 60,000
Corporate servers: MNE	~ 50,000	€ 46,000
Corporate server: SME	~ 35	€ 150

From these field data on actual expenses it can be derived that the cost of spam defence averages to € 1 per mailbox for both ISPs and large corporations.

Small and Medium Enterprises who operate their own mail servers run up a slightly higher annual cost of approx. € 5 per mailbox per year. This is due to the need to purchase and depreciate mail server plug-in tools that allow filtering. These tools are in practice integrated with the function to perform virus scanning, which is more in demand, and those costs are not part of this study's assessment. We therefore ascribed one third of the average plug-in cost per mailbox[37] to spam filtering.

Table 4-2 *Annual cost of server based spam defence for the Dutch market*

Market segment	Cost per mailbox / year	Segment size	Total direct Cost
Consumers	€ 1	9 million	€ 9 million
SME ISP	€ 1	1.5 million	€ 1.5 million
SME (own server)	€ 5	1.5 million	€ 7.5 million
MNE: (own servers)	€ 1	2 million	€ 2 million
Total NL		14 million	€ 20 million

Table 4-2 shows the cost on a national scale for the consumption of infrastructure resources. The number of mailboxes per user is higher in the SOHO and SME segment, but Smells operating their own mail servers incur higher costs, which is mainly due to the smaller economies of scale.

The total cost in the technical plant is rather low for a casual observer, compared to the Dutch ISP's annual turnover which is in the range of € 1.5 billion in 2004. Compared

[37] Most mail server plug-in vendors have site licenses that depend on the number of mailboxes.

to the profits most ISPs are making it often is (deletes) the profit. Most of the ISP's turnover is spent on Internet access infrastructure (broadband access an dial up traffic) and purchasing international upstream bandwidth. In 2001, when spam was still a minor problem, the market price for a large scale outsourced e-mail service was *f* 3.50 (~ € 1.60) per mailbox per year. This shows that the high amount of spam today has doubled the annual cost of e-mail services for the Netherlands.

A number of ISPs have provided us with cost figures that all come down to the current average cost of € 1 per mailbox per year. This however is for a case where only a part of their customers (roughly 35%) have activated spam filters. Some ISPs responded to our findings, with their observation of a current rapid growth in spam filter activation by their customers. This requires them to further invest in servers and anti-spam technology to serve that demand, a costly effort when the spam filter is included gratis with e-mail service for commercial reasons. Spam filtering is thus not a one off investment but an ongoing spending for ISPs.

4.3 Substantial policy and monitoring costs

The Dutch Government is also suffering from the increasing costs of unsolicited bulk e-mail for promotional ends. Besides the cost for enacting spam legislation and making policy, an ongoing cost is now incurred for monitoring and enforcing it by imposing administrative fines. In the Dutch system of sector regulation, all the supervised companies in the sector pay OPTA's costs. The bill for monitoring spam and enforcing spam legislation is thus passed to the industry.

Currently OPTA has a team of 5 full-time-equivalent working on the newly assigned task to monitor unsolicited e-mails promoting commercial, political or charitable ends. It has assigned two teams (each consisting of two employees, a detective from the *digital police* forces and a co-ordinator). Active since May, this years cost will be € 280 thousand. In the next year it shall rise to € 500 thousand. There have been cases in which conflicts with some spammers resulted in (Distributed) Denial of Service Attacks and Joe Jobs[38]. Some victims reported these to the police.

OPTA has received 3568 spam complaints since May 2004[39]. It has decided to concentrate on complaints regarding large-scale offenders. The Telecommunications Act allows OPTA to impose an administrative fine to a maximum of € 450,000. On 13 October 2004 Webwereld[40] published that SNK Bedrijfssoftware, one of the more

[38] Forging the originating address in an embarrassing spam to defame another

[39] These complaints are split in 90% spam, 8% unsolicited SMS-messages and 2% junk faxes and automated telephone calls. Status at OPTA, October 22, 2004

[40] Maarten Reijnders, Telecomwaakhond maakt jacht op spammers, http://www.webwereld.nl/nieuws/19742.phtml

notorious senders of unsolicited bulk e-mail, sought legal assistance after being visited by the OPTA spam team.

On the other hand the Government also sees a reduction of legal costs as its Courts are less burdened with private litigation. These may however go up when administrative fines by OPTA are challenged.

The decreasing number of Dutch spamruns directed at Dutch citizens has already shown that the new policy is effective in deterring some of the spammers.

4.4 Most costs are due to the international problem

From the various cost analyses provided in this chapter it is clear that ISPs and end-users spend millions to handle spam. However, their main costs have foreign sources. In Table 4-3 we resume the various cost we explored in the former sections. In this table we list the social cost of reduced reputation for companies and diminishing trust in the Internet as a viable channel for transacting (e-commerce) and costs due to spam annoyance as *pro memori*, as they cannot easily be quantified, but must not be overlooked.

Table 4-3 *The cost of spam without and with counter measures taken*

	Without any anti-spam actions	**With countermeasures**
Loss of social trust & annoyance	p.m.	p.m
Productivity loss	€ 1,667 million	€ 83.3 million
Extra Dial up cost	€ 21 million	€ 10.0 million
Spam-filtering:		
• Client based programs		Ca. € 2.0 million
• Server based incl. staff		€ 20.0 million
Bandwidth	€ 9,000	€ 9,000
Defining policies		€ 0.2 million
Monitoring & Enforcement		€ 0.5 million
Cost of spam in NL	€ 1,688 million	€ 116.0 million

We provide two cases. We list the Dutch productivity loss and consumer traffic (download) cost of spam in the first column, when no anti-spam actions would have been taken. These social costs, imposed on those who do not want to participate in the transaction the spammer hopes to close with an unknown prospect, are the typical figures one receives from the Internet security and anti-spam industry. The second column, gives a more realistic picture of the cost spam imposes on society. We add the spam filtering costs of end users with client based filter programs, ISPs and mail server owners and the cost governance cost of policy making, monitoring and enforcement.

Some of those acts reduce the amount of spam that is flowing through the system and thus productivity loss and download costs are lower with counter measures applied.

The cost of spam sent to Dutch persons by Dutch organisations is low compared to the large foreign influx. OPTA indicated in our interview that it is also working on a case of a Dutch offender sending in a run millions of spam abroad (via a mail server installed at a North-American hosting site). However, collaboration with other countries to prosecute cross border is still in its infancy.

It is understood that hard core spammers observe a relatively low cost barrier for sending unsolicited bulk e-mail, but a number of notorious offenders seem to have been deterred already by the institution of a legal framework that allows OPTA to levy administrative fines on offenders. To compare the burden, tabulated above with the cost of spam senders, we look in the next section after the cost incurred by the senders of unsolicited bulk e-mail and legitimate bulk e-mail.

4.5 Senders' costs are relatively low

People and organisations that send bulk e-mail do incur costs. These costs differ considerably between senders of spam through proxies and senders of bulk e-mail that use a service agency or deploy their own systems. In this section we will distinguish the two.

4.5.1 Costs incurred by a hardcore spammer using proxies

Send-safe is mentioned as the most used tool today to send spam. The company charges US$ 199 for a single copy of the program, but the sender also purchases credits that are counted down with each e-mail that is sent successfully. Table 4-4 shows the volume table.

Send-Safe users can use a list of proxies which is automatically downloaded by the program. Such a list typically consists of a few hundred machines. Users of the program can also add their own proxies, which are either found with a proxy scanner or purchased from a spammer. According to USA Today a list with 20,000 proxies sells in the range of US$ 2000 to US$ 3000 [41]. Prices have doubled since the summer of 2003 as The Register reported US$500 for a BotNet with 10,000 zombie-PCs[42].

[41] http://www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieprice_x.htm
[42] http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/

Table 4-4 *The cost for Send-Safe is less than US$ 0.000125 for each spam message sent*

Number of credits	Working period[43]	Price (US$)	Price per 1 million credits
400 000	30 days	$50	$125
1 000 000	30 days	$100	$100
3 000 000	30 days)	$200	$66.66
10 000 000	60 days	$400	$40
40 000 000	60 days	$800	$20
100 000 000	60 days	$1500	$15
150 000 000	60 days	$2000	$13.33
300 000 000	90 days	$3000	$10
Unlimited, one's own proxies or direct	30 days (no free extension)	$499	-

Apart from these set-up costs, someone who intends to send unsolicited bulk e-mail needs to acquire addresses. Addresses for unsolicited bulk e-mail are sold at relatively low prices. FXStyle.net sells a CD-ROM with 238 million addresses for US$ 29.95. These are of low quality, as they contain many addresses that have stopped functioning. Spammers have to apply an e-mail address verifier to clean up the list, which requires quite a lot of time if it is to be done without attracting suspicion. Good quality recent e-mail addresses command a high price. Specialising on a specific country also commands a premium. In the second half of 2003 R. van der Wal, from Apeldoorn, the Netherlands, offered via unsolicited bulk e-mail a CD-ROM with 10 million Dutch e-mail addresses for € 399. On June 24 an AOL systems engineer was arrested for selling the screen name database of more than 90 million names to a spammer for US$ 100,000.[44] In this non-representative but high-profile case the rate was USD 0.001 for a fresh e-mail address.

Finally a would-be sender of unsolicited bulk e-mail through a zombie PC network should not overlook the cost of network access. Sending a substantial number of e-mails requires a broadband connection of considerable upstream bandwidth. A DSL-link with an upstream bandwidth of 640 kbit/s can be used to send several hundreds of thousands of e-mail messages of less than 1 kB in size per hour. This will cost € 50 to € 65 per month. If not all addresses are correct the rate will fall back to several tens of thousands per hour, due to latency[45] effects. This means that a sender of unsolicited bulk e-mail who lacks high bandwidth (10 - 100 Mbit/s) Internet access does indeed need 30 days to use up 1 million Send-Safe credits.

[43] Free period extension unless otherwise indicated
[44] AOL customer list stolen, sold to spammer, http://www.msnbc.msn.com/id/5279826/
[45] The time needed to make contact and receive a response for conveying a packet to the destination server.

Most items thus can be purchased per month for several hundreds of US$. Depending on quality of *proxy lists* and *addresses* the prices can go up to several thousands US$. Senders of spam that would send millions of e-mails in a few hours need the co-operation of rogue hosters with access to very high bandwidth.

Based on the observed prices we can estimate that the aggregate of hard core spammers, responsible for the far majority of 145 million incoming e-mails per day in the Netherlands, are spending an amount of US$10,000 per day to reach potential Dutch customers, equivalent to 0.001 dollarcent per message. Senders of spam thus spend in the range of € 4 million per year to reach potential Dutch clients.

Interviewed parties were unable to provide a precise indication of the volume of unsolicited bulk e-mail campaigns from Dutch spammers directed at Dutch citizens and corporations. The typical Dutch spamrun seems to be in the range of several tens of thousands of e-mails, and lasts a few hours. The number of monthly Dutch spamruns reported to spamvrij.nl (see also Figure 3-3) have fallen to less than 60 per month, an average of 2 per day. This means that the combined group of hard core spammers in the Netherlands that deploy open proxies to attempt to reach Dutch citizens with unsolicited bulk e-mail incur direct monthly costs of a few hundred Euros.

4.5.2 Costs incurred by an organisation using a service agency

Corporate users that plan to send a mailing for promotional purposes can either install a bulk e-mail system or hire an e-mail marketing service provider. According to the DDMA the typical size of an e-mail campaign in the Netherlands lies between 10,000 and 150,000 e-mails. For these campaigns mail senders pay between € 15,000 and 30,000. About € 10,000 is used for project management and developing a campaign strategy. Several thousands of Euros are spent on creating the e-mail. Sending the bulk mail costs approximately € 100 for 1000 e-mails.

The DDMA does not have hard figures for the total amount of money spent in the Netherlands on e-mail marketing. In their view e-mail marketing ranges from contacting clients and (business) relations by newsletters and mailing lists to sending promotional offerings through the e-mail. A rough estimate is an annual spending of between € 125 and € 150 million.

In a recent edition of Bizz, the SME oriented business magazine,[46] an overview was presented of the services and possibilities of selected e-mail marketing application service providers and do-it-yourself bulk mail software. In the article prices are published of two e-mail service agencies, Blinker-Mailplus and Veritate MKB-Mail. It

[46] Fred Theunissen, *Bulkmail* , Bizz, 24 September 2004, pp. 57-63, Reed Business Information

is standard practice of e-mail marketing agencies to request a connection fee and an annual subscription, while charging staggered prices for different volumes of e-mail.

Mailplus can be considered cheap with its annual subscription fee of € 695 and annual volume charges of € 480 for 5 thousand e-mails up to € 1980 for 120 thousand mails. Veritate uses a linear pricing model. Their annual subscription includes the first 10,000 outgoing e-mails and they charge € 15 per thousand e-mails above the threshold.

These application service providers seem to cost less than the example calculation by the DDMA, but some caution is needed. . Prices in the Netherlands vary between a few and 40 Eurocents per address for mass groups and highly targeted groups such as medical doctors or judges. The address owner rents these addresses out to the mail sender for a specific mailing. Seen in this light it is clear that the AOL systems engineer arrested for selling customer screen names did so far below the going market rate.

The majority of the costs in bulk e-mail campaigns are not spent on sending the e-mail itself or on the supporting IT infrastructure, but on the marketing strategy, the project management stage, the creative effort and address acquisition.

4.5.3 Spam supermarkets

As there are service bureaus for e-mail marketing that operate on the legitimate side of the business, some hard core spammers have mimicked this for their spam business. These are called *Spam Supermarkets*. Anti-spam organisations, like Spamhaus, have located several of these supermarkets operating from China. The spam supermarkets sell all the products and functions needed to send out a spamrun. One can hire the tools, *bullet proof webhosting*, access to their networks and access to Botnets of ZombiePCs. For those who want to send out really large spam runs (millions of mails in a few hours) botnets are often too slow and they sell temporary access to a spam mail server in a datacentre linked to a Tier 1 internet backbone. Some of these Tier 1 Internet backbone providers are still willing to co-operate with these ventures. In particular when they are in administration (Chapter 11 bankruptcy restructuring) a client willing to pay a million dollar a year is attractive.

The people behind spam supermarkets also engage in spam related trades of (stolen) credit card numbers and phishing scams (identity theft solicited via fraudulent and deceptive e-mails). According to various interviewees, Spamhaus and Symantec, a number of the known Hard Core spammers are also the persons behind the release of most computer viruses during the last two years, that were a means to create the *Botnets* of ZombiePCs they sell access to by the hour.

4.5.4 A ten- to hundred thousandfold cost difference for spam

Observing the orders in magnitude differences of 0.0001 -0.001 dollarcent per message and 20 - 150 Eurocent for a legitimate campaign, the question remains whether the new legal framework is sufficiently deterring to diminish spam. The attractiveness of spam may lure new offenders to rise to the occasion, in which case monitoring and enforcement may become a 'whack-a-mole' effort. In the next chapter we will therefore explore the incentives for spammers by assessing the business case for spam.

5 The business case for spam

In understanding the business case for spam, it is important to realise that the aggregate cost per product unit sold (or customer, member or donor acquired) is not necessarily substantially lower than other, more mainstream means to deliver promotional information. Various flavours of unsolicited mail and calls have proven to be an alley for organisations that are unable to convey their message through regular (mainstream) media. In other cases senders of unsolicited messages prefer the addressed contact that allows them to fine-tune campaigns far above the quality of advertising media.

The main issue is the cost relating to customer acquisition and sales. In this chapter we describe the value chain for spam and compare it with direct marketing. Then the typical products and services offered in national and international spam are compared. We then focus on essential differences between an opt-in direct marketing system and spam. We elaborate on the consequences for spam effectively going underground to acquire access, and conclude with the profitability of the value chain and options for intervention.

5.1 The value chain and costs of spam

People sending spam today need to buy or create five inputs before they can start their business. Figure 5-1 repeats the chain of technologies and systems we sketched at the end of Chapter 3. With the findings on the costs various actors face, we are now able to look after the business case for spam.

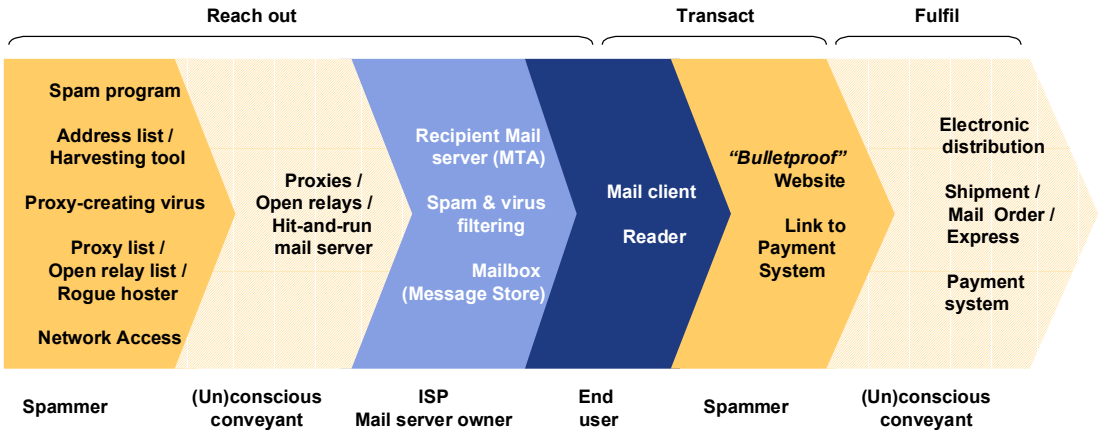


Figure 5-1 *The chain of technologies and systems involved in a spam transaction*

Senders of spam need to purchase a spam program like Send-Safe or Dark Mailer. To operate the program they need access to a mail server or *proxies*. In most cases *ZombiePCs,* hacked or virus infected computers that have been transformed into

hidden spam gateway without consent of the owner. To create them some spammers release *proxy-creating viruses* on the Internet. To reach potential customers they need to buy an e-mail address list or a harvesting program that will search the Internet for addresses. For sending messages to the proxies network access, preferably broadband, is needed. To collect potential customer replies a "*Bulletproof*" website is handsome. As a potential input one could count a contract with an on-line payment system to conclude the transactions, but this part of the transaction can also be handled off-line, depending on the nature of the good or service sold. In a similar vein not every sender of spam, planning to use Zombie-PCs need access to a skilled virus writer or engage to release one on the Internet. Access to someone who has performed that act and sells usage time of a network of *proxies* (a *Botnet*) suffices.

The profitability for the business case of senders of spam depends critically on their customer acquisition costs and reach. The barrier of entry for a hard core spam run is still relatively low, it requires up to € 1000 to start with a relatively high quality list of addresses as can be derived from the data supplied in section 4.5. Intervention can be directed both at one of the five inputs senders of unsolicited bulk e-mail need and their reach to recipients that determines the customer acquisition cost in the business case. Interventions can have the goal to deter entry, deny access to essential inputs or raise their cost to submit a high volume of unsolicited e-mail to end users.

When spammers are able to convert 1 customer out of every million messages they sent, they bear a customer acquisition cost of US$100. This takes the price list of Send-Safe as a reasonable departure point for the cost per message sent. If a spammer is able to sell its proposition on a prospect per 10,000 outgoing e-mails, its customer acquisition cost falls to US$ 1 per customer.

5.2 A comparison with Direct Marketing

For assessing the business case, spam is best compared with the case for direct marketing. Direct marketers claim success rates for e-mail marketing far higher than via conventional postal mail. The customer acquisition costs for a campaign via postal mail is in the range of € 80 per win. For e-mail it falls, due to higher response rates, to a few Euro.

Legitimate senders of bulk e-mail incur campaign costs that rapidly rise above € 0.20 per e-mail, depending on campaign size and the specificity of the e-mail address rented (where prices vary between € 0.04 - € 0.40 per address). The DDMA estimates the total spending of their sector on e-mail marketing in the Netherlands at € 100 - € 125 million per year. They can easily bear costs up to € 0.50 per message sent.

When we calculated the direct cost incurred by hard core spammers to send their 145 million mails per day to Dutch receivers we end up at a cost level of ca. US$ 15,000

per day or € 4 million per year. This demonstrates that in financial size spam has a considerable cost. It suggests that hard core spammers must be able to realise a turnover of more than € 10 - 20 million per year on the Dutch market to earn back their spam, product and shipment costs.

Our comparison informs us that a sender of spam observes customer acquisition cost that are regular in Direct Mail business practices if he is able to transact with a customer out of ten thousand to one million send spam messages. This low level of required success rate to cover cost makes it rather though to raise the cost a sender of spam observes in reaching out to recipients by installing spam filters in between. Filters needs to reduce the successful prospect conversion rate with a factor 100 to 1000 to make the business case for spam unprofitable except for the most expensive goods. Most good filters reach to 90% to 95% successful spam detection, a mere 10- to 20-fold reduction. A detailed comparison with direct marketing can be found in Annex B.

5.3 Typical products offered

International spam offers various life-style drugs, mortgages, adult entertainment, money-making schemes, etc. Dutch spam is quite different.

The overview of the sales subjects of all Dutch spamruns[47] filed to spamvrij.nl over the past 365 days indicates a shift to business products and services since the new Telecommunications Act came into force in May. However, Dutch spam had a rather business-like nature even before then. Never have adult entertainment services or websites been promoted to Dutch citizens by a Dutch written spam message. This orientation on business products has led to a change in the economics, as the addressable market has been diminished in size.

This disadvantage for the sender is partly countered by the fact that it sending commercial messages to businesses is legal. The transaction size is also large in the business market. It causes one is willing to accept a different success rate. Also spam-filters, in particular the high quality statistical and adaptive ones, are easily passed, as Dutch language spam is such a rare event it is not recognised in most filters.

5.4 Acquiring customers' addresses

The harvesting of e-mail addresses and the selling of address CD-ROMs is a key phenomenon that distinguishes the business case for spam from legitimate practices in which bulk mailers use an opt-in list. There are differences in the control that the address list owners have in what is done with their lists.

[47] http://www.spamvrij.nl/lijsten/lijst.php?type=run&show=minimal&stat=Geel

Many large Dutch address lists owners rent out their mailing lists through a listbroker. These owners can be commercial organisations or non-profit organisations with a very large membership or group of donors. It is frequently disputed whether these address data really are opt-ins, which would allow offerings of third parties.

The trade in e-mail addresses of large established businesses differs considerably from that of Mail Harvesters and traders in e-mail address CD-ROMs.

The quality of an address database depends on its accuracy and recency. As a consequence large organisations have a daily updating routine. An association with 4 million members on average tracks 250 thousand (physical address) moves per year in its database, which comes down to about 1000 per work day.

Large (not-for-profit) corporations rent out their addresses, but maintain contractual control by using single-right-to-use contracts. Fulfilling an intermediary role, listbrokers maintain a regularly updated copy of address lists of their contract partners, but in their operations for a third party they do not insert or match addresses without consent of the owner.

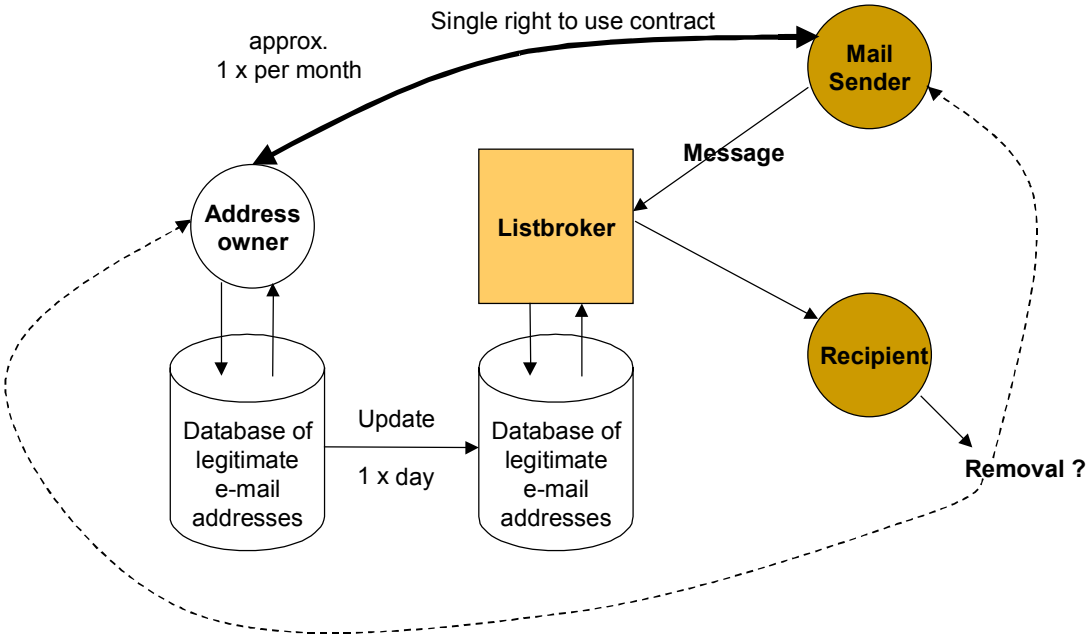


Figure 5-2 *Listbrokers allow mail distribution without handing over the address*

In an opt-in regime the client once has to provide permission to the address owner once. However, users who receive mail (either postal or via e-mail) are often unaware of where to turn to remove their name from the list. The DDMA is pleading for a transparency rule. Every outgoing mailing should state: "We have received your e-mail address from *organisation X,* whom you have authorised for third party mail". The

recipient would then know where to opt out. This is not common practice so recipients are usually unclear about the source of the e-mail address.

An essential difference between spammers and legitimate senders in the handling of address lists lies in the fact that the circles are closed in legitimate renting of opt-in addresses and listbrokers need to update very regularly.

- In the spam industry all circles are open.
- Once the e-mail address has been harvested, it will continue to circulate on all kinds of CD-ROMs which are endlessly multiplied and sold.

The standard business practice is thus renting out address lists per specific bulk mailing with prior consent and control of the owner. This differs from the practice in the spam industry, where the lists are traded as goods and are copied endlessly.
This very different behaviour in handling[48] address files provides thus a legal intervention point to make a spammer vulnerable for the law.

5.5 Acquiring network access

Another difference between legitimate senders of bulk e-mail and senders of spam lies in their different approach to acquiring network access. Legitimate senders and e-mail marketing service providers install and operate their own servers on a fixed IP-address. In their need to hide from spam blocklists, spammers buy underground access to networks for sending spam through zombie PCs or deploy dynamic hit-and-run tactics. This part of the technology race is well documented.

It is less documented that they require far higher stability to collect the responses. The websites often circulate between bullet-proof webhosters in China, Korea or Russia. They also receive new domain names regularly. Although everything looks dynamic the domain name server is often a far more stable element of the spammer's infrastructure, and this opens up possibilities for the detection of his affiliates.

5.6 Deterrence and intervention points in the value chain

Prohibiting sending of unsolicited bulk e-mail by law is a deterrence to would-be spammers. The risk to be caught and fined introduced by law raises the risk-level of the prospective spam venture and thus makes the generic business case less attractive. General fines are not a specific intervention in a part of the value chain, but deter entry into this business. Spammers, becoming more fearful of enforcement, tend to hide their tractability and avoid detection[49] by technical, physical and legal proxies like zombie-PCs, remote operations in obscure locations and use of strawmans. As long as in the

[48] 'Verwerken'; the Dutch legal term in the privacy act.
[49] E.g. false senders, proxies and rapid alternating domain names for response websites

view of hard core spammers the chances to receive a fine is low, even with high fines in the books, deterrence does not influence the business case to a substantive level.

In this section we will summarise the findings of our value chain analysis for potential intervention points to make the business case for spam less attractive. As discussed in the former sections, the profitability for the business case of senders of spam depends critically on their customer acquisition costs and reach. The barrier of entry for a hard core spam run is still relatively low, it requires up to € 1000 to start with a relatively high quality list of addresses. Intervention can be directed at a number of inputs senders of unsolicited bulk e-mail need and their reach to recipients that determines the cost in the business case. Interventions can have the goal to raise their cost to submit a high volume of unsolicited e-mail to end users.

We have found the following potential intervention points to damage the business case for sending spam:

- Purchasing a spam program
- Control over (a list of) proxies or access to mail relays or servers
- Buying or harvesting e-mail addresses
- Network access
- Bulletproof webhosting
- The financial payment system
- The cost of reaching out to recipients
- 'Willingness to buy' of a recipient
- Skills to release Zombie-PC viruses

Assessing the business case for spam, a key effect of the technology race has been that hardcore spam is filtered and blocked to such an extent that it has become lucrative only in very large volumes. Several persons we interviewed doubted that sending spam is really all that profitable. It may remain a fringe business that just manages to survive and might just require a small economic nudge to fall through. This opens up possibilities for economic countermeasures. Making spam expensive would be the way to invalidate the business case, but costs per mail would have to rise 100 to 1000-fold. Our comparison with the case for direct mail (by post or by e-mail) show that legitimate senders of bulk e-mail can bear cost of a few eurocents per message, so this is a potential intervention point in the value chain. The question is if the consumer is able to bear that cost.

There are other potential intervention points as well. There is for instance a clear difference between renting an address list in a single use license and purchasing an address list. This might be used in legislative finetuning.

Another road is to focus on spammers' access points to the Internet. These points are difficult to find as access is gained partly in foreign countries and partly over links with virus makers. It would require installing *honeyproxies* for investigation and prosecution evidence. With a *honeyproxy* one becomes able to find the real IP-address

where the spammer has gained network access and it may become possible to find out who controls the zombies and (re)sells them.

We think it will be very difficult to prohibit the sale of spam programs, and therefore we do not elaborate on it.

A more promising approach seems to be intervention in the response chain. After all this is a far more stable area, as a spammer cannot move away in seconds (which can be done in zombiePCs) but requires days or weeks to collect responses. It requires looking at the *Bulletproof* webhost, but also a deeper look into the payment system may be instructive. For some services on the Internet (e.g. adult entertainment) credit card companies require much higher collection fees, due to shirking risk, than for selling books etc.

In the next chapter the current countermeasures are described per category.

6 Current countermeasures taken per category

Several countermeasures are taken per category. These include legal, technological, social or organisational and economical countermeasures. Different user groups, such as end-users, industry, legitimate senders and the Government, take different measures. A combination of countermeasures is always required as there is no single solution for the spam problem. And because these (combinations of) countermeasures and the groups/users applying them are not complementary (the groups have not yet closed ranks'), no measure has yet proved sufficiently effective.

6.1 Technologies for blocking and tagging

Several technologies are used for blocking or tagging spam. Both end-users and ISPs are taking measures. End-users can use a spam filter on their computers. A drawback of this solution is that all e-mail is transferred to the user's computer, so it still uses bandwidth. Moreover, end-users cannot keep up with the arms race because spammers keep finding tricks to circumvent the filtering techniques. Finally filtering is only partly effective and tackles only part of the spam problem. ISPs can use spam filters on their servers. In that case only legitimate e-mail is transferred to the user's computer (though with a risk of false positives).

6.1.1 End-users and ISPs use filters

The use of spam filters to separate legitimate e-mail from spam is only partly effective and tackles only part of the spam problem. A spam filter is a piece of software that blocks or tags an incoming e-mail based on its content. Content is marked as spam with a certain *probability*. The probability parameters are obtained by statistically analysing hundreds of known spam e-mails and legitimate e-mails. Therefore spam blocking is not always convenient, and tagging is offered instead.

Blocking

As e-mail is marked as spam with a certain probability, automatic discarding of e-mail marked as spam is not a straightforward solution. In most cases ISPs leave the decision to use a spam filter to the customer. The customer can choose which filtering level he wishes to use and what to do with an e-mail marked as spam. Users can specify to block all e-mail from specified countries, such as China or Russia. In general, filtering methods are customer-specific.

Tagging

Corporate users are concerned about automatic blocking of e-mail. Some corporate IT departments only offer 'probably spam' tagging instead of blocking. The user can read or discard the tagged e-mail himself. A drawback of this method is that users still need to inspect all e-mails to see whether they are legitimate or spam.

6.1.2 Whitelists

Whitelists are lists of IP addresses, domain names, email addresses or the contents of the headers or the body, or a combination of these , that can be used to decide if a certain party can be trusted. Consumers may compile personal whitelists of e-mail addresses. E-mail from these addresses is always accepted, even if the spam filter decides that the message is spam. ISPs use whitelists to accept all mail from trusted parties, such as other ISPs. The use of whitelists reduces the processor load because the mail server does not need to scan that part of the incoming e-mail anymore.

6.1.3 Blacklists used by ISPs to block spam

Blacklists or blocklists are lists of IP addresses, domain names, email addresses or content of the headers or the body, or a combination of these, that can be used to help identify spam. Various ISPs, bandwidth providers or consumers subscribe to these blacklist databases in order to be able to filter out spam sent to their network, subscribers or mailbox. The databases are usually maintained by organisations that process large amounts of e-mail. Table 6-1 provides an overview of the different categories of blacklists together with some examples.

Table 6-1 *Blacklists appear in various flavours*

Category	Clarification	Example
spammer lists	Lists containing IP addresses used for sending spam	Spamhouse Block List (SBL), a real-time database of IP addresses of verified spam sources
Open relay lists	Lists containing IP addresses of servers which have to possibility to relay mail	ORDB.org, a real-time database containing IP addresses of open relays
Open-proxy lists	Lists containing IP addresses used for sending spam by zombie PCs	Spamhouse Exploits Block List (XBL), a Real-time database containing IP addresses of known exploits including open proxies
spam domains lists	Lists containing domains referred to in spam	Spam URL Realtime Blocklists (SURBL)
Virus source lists	Lists containing IP addresses used for sending spam	Virbl.bit.nl
Phishing sources	Lists containing hand-confirmed IPs and URLs of fraudulent websites designed to fool recipients into divulging personal financial data	Included for now in ‘multi.surbl.org’ because the list is small
Combined lists	Lists containing other lists	Multi.surbl.org Rbls.org

spam domains blacklists
Spam usually offers a product or service through a website, presented as a hyperlink, or URL, in the e-mail. Dutch ISP Multikabel has constructed a blacklist named SURBL with domains that offer these products or services. The receiving e-mail server blocks or tags e-mail as spam when these domains are present in the body of the message.

Open-proxy lists
Today, most e-mail is sent by open proxies or zombie PCs. An open proxy is a PC that is configured as an e-mail server. It is usually a virus that is responsible for turning the PC into an e-mail server. The open proxy is controlled by a virus writer or spam sender, who can upload a spam e-mail and a list of addresses to the open proxy. The open proxy starts sending e-mail without the PC owner knowing about it.

Open relay lists
Mail servers used to have a standard configuration as mail relays to serve as smart hosts for other mail servers in other domains. Open relays are mail servers that accept e-mail from other domains to other domains. Today configurations do not allow relay because open relays are used by spammers as access servers. Relaying is not necessary because the Internet is stable and allows every mail server to reach every other mail server.

Virus-source lists
Today spam is mostly sent by zombie PCs created by viruses that are usually spread by e-mail. A virus-source list contains IP addresses of hijacked computers that send e-mails with these viruses. ISP's mail servers check incoming and outgoing mail for viruses. If an incoming virus is detected, the virus is removed before the message is forwarded to the end-user. The IP of the sending server or computer is placed on a list and further mail from that IP is not accepted. This prevents the receiving computer and other computers from being infected by a virus that could turn them into zombie PCs.

If a computer is hijacked through a security leak and software is illegally uploaded to the computer to send viruses by e-mail, the server for outgoing mail will notice that virus and will not accept any more e-mail. Again, the IP of that computer is put on the list for other ISPs.

Finally, viruses are mainly a regional problem because they are spread by email using the local address book. Regional creation of zombie PCs can be prevented by the use of virus-source lists.

6.1.4 Legitimate senders are verified

Before accepting an e-mail the ISP verifies the domain of the sender’s e-mail address. If the domain does not exist the e-mail is rejected. A major drawback of this technique

is that the sender himself can specify that e-mail address very easily. The sender can provide someone else's valid return e-mail address to avoid detection. This technique is called spoofing. Tentative countermeasures against spoofing that currently receive much attention are listed below. These countermeasures still have to be investigated in the context of the topology of communication in the future. This context is characterised by a common vision that users are connected anytime and anywhere. Today these systems perform an important function in static or corporate environments.

Sender Policy Framework

A countermeasure against spoofing is called Sender Policy Framework (SPF). Using SPF, the receiving server can verify if the sending server is permitted to send mail for the domain entered on the message *envelope*. Domains participating in the SPF programme publish their sending mail servers in an SPF record that is published in the Domain Name System (DNS). Receiving mail servers can check the SPF records and compare the domains. SPF is a good countermeasure against spam sent by zombie PCs. A drawback of this system is that spammers can register a domain, publish an SPF record and start sending spam. Spam filters will then give extra points for a positive SPF check, which increases the chances of spam reaching the end-user. Nevertheless, if one publishes an SPF record the registered domain is visible in the spam header. The domain is linked to personal and financial data by the registrar and the spammer may be identified. In the Netherlands only 221 domains are registered in the SPF (Table 6-2). This is very low compared to the registration of 26,596 domains of Luxembourg[50].

Table 6-2 *.nl, nr. 3 country code top level domains rank low in SPF registrations*

1	.com	87059	**11**	.uk	1434	**21**	.it	227	**31**	.es	85	**41**	.gr	43
2	.lu	26596	**12**	.us	875	**22**	.nl	221	**32**	.cc	83	**42**	.bo	35
3	.ch	19527	**13**	.br	709	**23**	.edu	167	**33**	.fr	70	**43**	.cl	32
4	.net	7718	**14**	.ca	548	**24**	.se	136	**34**	.pt	66	**44**	.mx	30
5	.org	5142	**15**	.dk	384	**25**	.nz	130	**35**	.nu	63	**45**	.jp	30
6	.pl	4476	**16**	.ru	348	**26**	.be	129	**36**	.name	58	**46**	.ar	27
7	.de	2496	**17**	.za	342	**27**	.hu	111	**37**	.fi	56	**47**	.hk	25
8	.ua	2348	**18**	.info	341	**28**	.ro	108	**38**	.tv	54	**48**	.gov	22
9	.au	2323	**19**	.at	341	**29**	.no	102	**39**	.ws	50	**49**	.ie	22
10	.aq	2033	**20**	.biz	296	**30**	.cz	91	**40**	.cx	46	**50**	.ee	21

[50] http://spftools.infinitepenguins.net/register.php

Purported Responsible Address
A slightly different countermeasure against spam is called Purported Responsible Address (PRA). PRA is a part of Microsoft's Caller ID. Using PRA, the receiving server can verify if the sending server is permitted to send mail for the domain entered in the *header* of the message, which unfortunately is part of the body of the message. The algorithm to derive the sending domain from the header is covered by a Microsoft patent. Though the patent is free, a licence must be obtained to use the PRA.

Sender ID
Sender ID is a standard proposed by Microsoft that was merged from SPF and PRA using SPF records. In the Sender ID standard it is possible to check for a legitimate sender on both the message envelope and the body. The Internet community, using open standards which are inherently used in core Internet structure, has rejected Sender ID as a standard because the patent issues for PRA are incorporated in Sender ID as well. AOL, the largest ISP, has rejected Sender ID on the basis of its license terms. AOL continues to use only SPF.

6.2 Raising costs for senders

An important issue is to raise costs for senders. The business case for spam holds because a large number of e-mails can be sent with minimum costs. Though some steps are currently being taken to raise costs for senders, this is still very difficult due to the present cost model of mail. Customers pay per account, and not per e-mail sent.

Counting and throttling the number of sent e-mails
Spamming is attractive because a small response percentage to a very large number of e-mails is profitable when sending a high volume is still cheap and easy. ISPs are raising costs for customers who send large volumes of e-mail by offering them a business account instead of a consumer account. ISPs measure the number of e-mails sent by their customers. If it exceeds a certain threshold, the e-mail server stops accepting e-mail. In doing so the ISPs prevent spam and also protect their Fair Use Policy.

Raising contractual barriers
Spammers used to use dial-up connections to reach the Internet through an ISP. The lengthy dial-up time needed to send spam used to generate income for ISPs. Today, ISPs acknowledge that spam is harmful and they try to keep spammers from their networks. ISPs even add anti-spam passages in their contracts to raise contractual barriers.

Tarpitting
It is possible to configure a mail server to accept e-mail with an increasing delay for each email after a certain threshold. This raises the costs for spammers. Moreover, spammers most probably assume that the connection has stalled, and give up.

Private litigation
Some organisations even identified spammers and filed lawsuits against them. These spammers were prosecuted not for sending spam, but for the content of the messages. Prosecution for content instead of for sending spam may lead to much higher fines. Making spammers pay high fines ruins their business case.

Fining
In the Netherlands OPTA can impose an administrative fine up to € 450,000. This has already proved to have a deterring effect. The FTC is investigating the feasibility of an Informant reward system[51].

6.3 Social and organisational responsibility stressed

A key issue is to make responsible use of the e-mail medium. ISPs and e-mail hosters educate their customers to help them protect themselves against spam. Customers are educated with information on how to use their e-mail addresses and how to deal with spam. On the other hand, some companies send spam without knowing. Companies should be informed about the impact and regulations of sending unsolicited bulk e-mail. Spamvrij.nl publishes the details of companies that have spammed on a website. This appears to be a very effective way to prevent them from further spamming.

Customers must take care when supplying their e-mail address
Customers are advised to be careful when providing their e-mail addresses to organisations, companies and individuals. Their e-mail address is an easy prey for so called harvesters, who collect e-mail addresses from websites and Usenet. The customer must take care to verify that their e-mail address will only be used to send the information requested by the customer. Legitimate use can be verified by checking the possibility for removal of their e-mail address from the database and by checking if their e-mail address is being used by third parties.

End-users must not reply to spam
End-users should not reply to spam messages. A natural reaction for end-users who receive spam is to respond, asking the spammer to stop. However, this makes matters worse because it confirms to the spammer that the e-mail address is valid and active. The same goes for 'unsubscribe' links in the message body. Basically, end-users should not reply to a spam message in any way. This advice conflicts with legislation

[51] http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf

that requires spammers to provide an unsubscribe link in the spam message to be used by the recipient to opt-out from receiving spam.

End-users should not buy spam-offered products
End-users are advised not to buy any goods offered by spammers. Generating profit, spammers' ultimate goal , will only encourage them.

Companies or retailers should be informed if they sending unsolicited bulk e-mail
Some of the spamruns stem from companies that are ignorant to the definition of spam. These companies are unaware that their communication with (potential) customers is basically spam. They usually stop sending bulk e-mail when informed.

End-users are advised to report spamruns
End-users are advised to report spamruns. The OPTA and spamvrij.nl take action against spammers.

End-users are advised to secure their computers from being hijacked
A popular way to send spam is to use viruses to create zombie PCs. Proper protection against viruses guards against the PC being used to propagate spam.

Individuals are organising
People are organising in Usenet or newsgroups against spammers spamvrij.nl is a socially initiated organisation and is run by volunteers. At the moment their job is effective, but it is impossible for them to definitively end spam.

6.4 European and national laws are being written

EU directive 2002/58/EG deliberations 40-46 and Article 13 are implemented in the Dutch Telecommunications Act number 28851 as Article 11.7. According to Article 11.7 customers should be protected from receiving unsolicited bulk e-mail. OPTA enforces the Act and can impose fines on spammers of up to € 450,000. The Act has an opt-in model for consumers and an opt-out for companies. In the near future the Act will be changed to protect companies against spam as well.

Scope and nature of Act
The result of discussions in Parliament on the Telecommunications Act has resulted in the fact that today it is possible to legally send spam from the Netherlands to other countries. The nature of the Act allows this because the Act focuses on the recipients instead of the senders of electronic messages.

Consumers cannot be spammed, companies can
Article 11.7 of the Act protects consumers from receiving spam. It differs from the EU directive in that spam can be sent to companies. In the Netherlands natural persons are

protected by law, but legal persons are not. A subtle distinction arises because some companies operate as natural persons and others operate as legal persons. In this scenario companies seen as natural persons are protected from spam, but companies seen as legal persons are not. In practice it is very hard or impossible to distinguish between private and corporate e-mail addresses. After corporate addresses are selected, a second selection must be made to remove the organisations operating as natural persons.

A list of legal intervention points deployed in some of the Unites States
In the United States a number of States attempted to pass legislation on spam in the last decade, before policy shifted to the federal level with the enactment of the CAN-spam act. Besides difference in definition, these US-attempts provide us with a list of candidate measures to link further legislative interventions to:

- Opt-in
- Opt-out
- Honour remove request
- False sender address
- Use of third party domain name
- Falsification of routing information
- Clear identification of sender
- Misleading subject line
- Label
- Prior relationship / Consent
- ISP Policy

7 An improved toolkit of solutions to decrease spam

An organised approach is required to assess the various types of countermeasure that have been taken and that could be taken. Figure 7-1 on the next page sketches the general framework we use to categorise the diversity of countermeasures. A detailed linking of this framework to the improvements we describe in the next sections of this chapter can be found in Annex C.

In chapter 6 we followed this approach on categories that link them to the horizontal axis in the figure. In this chapter we will elaborate on several of these measures, but first we will turn to the vertical axis in the figure and look for gaps in the toolkit of countermeasures per user / stakeholder category.

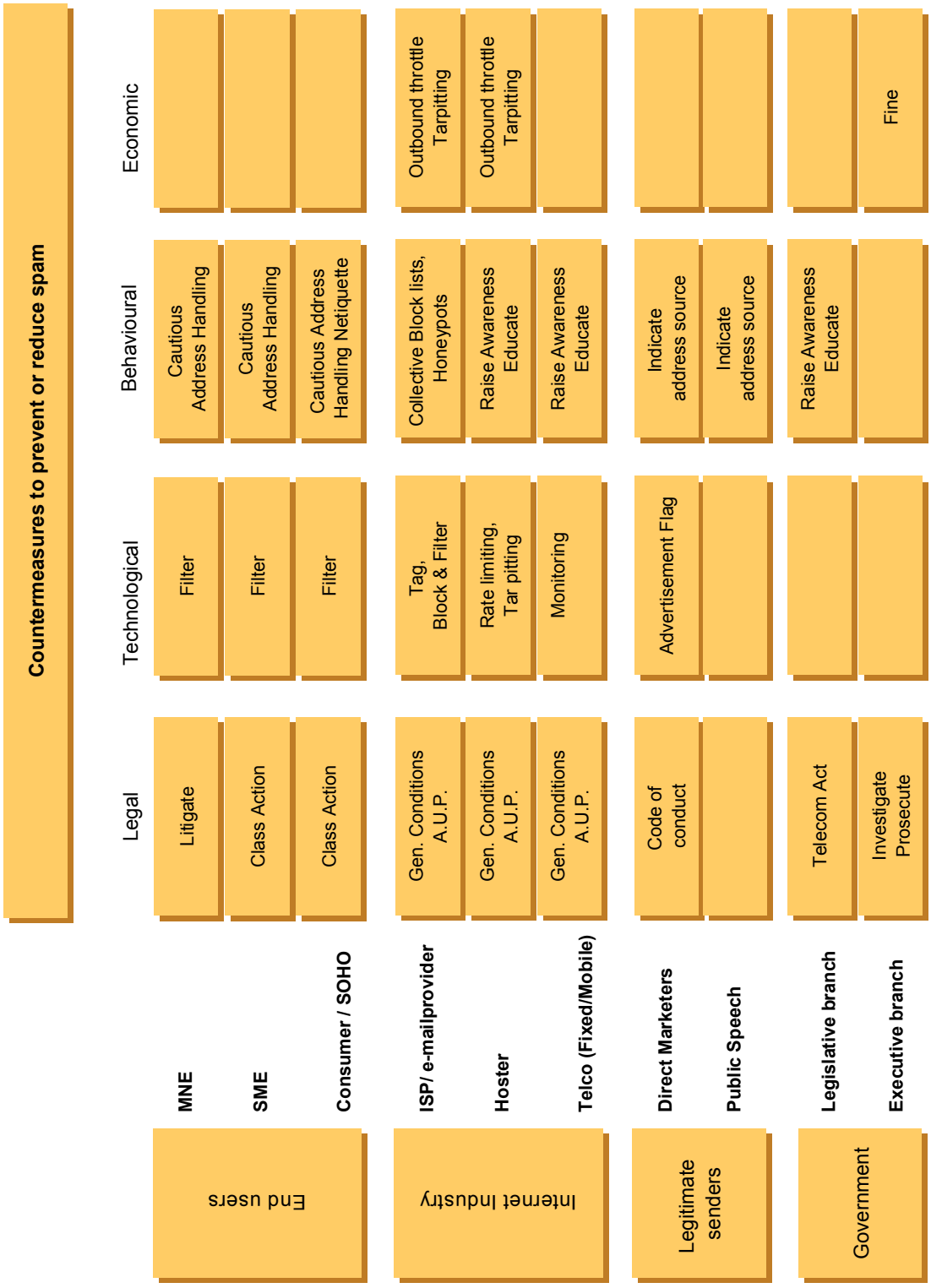
Clearly not all spaces in our framework are filled to an equal extent. The number of technological and social / organisational measures already taken is much larger than the current amount of legal provisions. It is particularly striking that the column for current economic countermeasures is empty.

It would be a great leap if an economic countermeasure could be introduced. Several proposals are circulating that include the introduction of an *electronic stamp* to shift the business case. In our interviews we received information on recent initiatives that may fill in some parts in this area of the toolkit. In several cases these initiatives are quite comprehensive and require complementary initiatives in the legal, technological and social / organisational areas. Such amounts of co-ordination require collective action since they often reach too far for (start-up) entrepreneurial organisations. Some components of these proposals have their own merits and can be introduced separately or as part of a bootstrapping effort.

In the next sections, we list in more detail existing and proposed countermeasures that can be taken by various actors, whom we categorise as *End-users*, *Internet Industry*, *Legitimate senders*, *Government*. We have disregarded the trivial additional case of ignorant spammers, for whom the countermeasure is to stop sending spam

7.1 End-users can reduce their vulnerability to spam

End-users can reduce their vulnerability by taking several countermeasures that are listed in this section.



Legend:

MNE = Multinational Enterprise

SME = Small & Medium Enterprise

SOHO = Small Office / Home Office

ISP = Internet Service Provider

Figure 7-1 *Categorising existing countermeasures for the toolkit to decrease spam*

7.1.1 Legal actions

End-users who wish to start litigation need to trace the spammer. However, it is not possible for businesses to file for damage compensation for lost employee productivity, because current Dutch legislation allows unsolicited automated bulk e-mail to be sent to businesses. This effectively leaves impersonation (identity theft), which can be traced by a sudden influx of bounces, and defamation (for instance for the use without consent of products and services of a firm's brand in a spam offer) as the main alleys for litigation.

- Businesses could adapt their general terms of trade with a clause stating that a buyer-intermediary is not allowed to promote their products and services through unsolicited bulk e-mail for resale.

Private litigation in Phishing-scams is more obvious for MNEs. They are characterised by the sender's intent to impersonate as a highly reputable firm with a large customer base with the goal to mislead these customers, consequently damaging consumer faith in e-commerce.

- Businesses are advised to at least start collecting material and maintaining files on various kinds of impersonation and defamation (such as *Joe Jobs* and *Phishing*) that may be submitted in Court when joining in a case against a spammer.

Private litigation against senders of spam is expensive even for MNEs. Small and Medium-size Enterprises can only effectively pursue this route if they join forces. The barrier for consumers and SOHO firms is even larger in this area.

- Employers associations and consumer associations could provide support or unite parties in collective Court cases (class actions) against spammers.

The cost and difficulties of litigation is one of the prime reasons consumer activists such as Spamvrij resorted to *naming, blaming* and *shaming*. They advocate the adoption of additional anti-spam legislation. The new Act also reduces chances for a collective court case route for consumers, as filing of the complaints with OPTA is required first.

7.1.2 Technological actions

The category of technological actions can be divided into actions against inbound messages and misuse of systems against outbound messages. We start with inbound messages:

- End-users can activate spam tags and filters provided by their ISPs

If this tool is not available or of insufficient quality they can:

- End-users can purchase solutions for their mail servers or mail clients
- End-users can install and configure stand-alone spam filtering equipment or plug-in tools for their mail server software (depending on size of company)

or

- End-users can install spam-filtering e-mail clients such as MailWasher etc.

However, activating spam filtering at the ISP or at corporate mail servers is recommended, since local mail-client spam-filtering does not reduce telephone bills for dial up users. This applies mainly to small businesses, employees in transit and working from home and consumers.

Spam filters can be delivered at different quality levels for less or more demanding end-users.
- End-users can install filters for the average user that add tags identifying spam in the subject lines in e-mail clients
- End-users can install personalised high quality filters, with low false positives for those employees who suffer from a large amount of spam. Deploying this requires end-user education.
- End-users can activate Challenge / Response filters with whitelisting (linked to *authenticated* outbound) as the most far-reaching technical solution.

Challenge / Response has its drawbacks as it increases e-mail traffic and requires the user to perform actions when unknown mail arrives in the filter because the legitimate sender does not understand the challenge. For this reason end-users should regularly check their mail for unknown sources that fail to respond to the challenge.

End-users should also become better aware of potential misuse of their PC or systems for mail forwarding (either zombie PCs or badly configured software).
- End-users should monitor their PCs or systems (more) frequently for (outbound) suspicious traffic or have the traffic monitored by the ISP
- End-users should be aware of the threats of viruses and adware / spyware in installing proxies, and secure their system with (personal) firewalls and anti-virus software if they have a broadband connection.

7.1.3 Behavioural (social and organisational) actions

To reduce their vulnerability to spam end-users could substantially adapt their behaviour in distributing newly minted e-mail addresses. Caution is a first step. MNEs and SMEs can introduce internal spam countering policies to alter behaviour, such as informing their employees to hand out e-mail addresses with care and caution, informing them not to respond to offerings in spam and opt-out, and how to file a complaint.

End-users are advised to:
- be careful when supplying their e-mail address
- to neglect incoming spam and avoid to respond or unsubscribe

- resist buying spam-offered products or responding to hoaxes or pyramid (Ponzi) schemes
- report spamruns to authorities and/or activist groups
- refrain from engaging in sending spam themselves.

An often better behavioural action is to educate companies or retailers about the effects of sending unsolicited bulk e-mail. Therefore, reporting complaints on spamruns to authorities or establishing activist groups who take further action is the recommended route.

7.1.4 Economic actions

Economic countermeasures by end-users are non-existent since e-mail is free of charge. However, there are several proposals to introduce electronic stamps. It is regularly stated that end-users will not want to start paying for outgoing mail, but some proposals contain incentives for end-users to pay when receiving or reading a mail. Users could put personal contacts and desired newsletters and mailing list subscriptions on a whitelist that allows free entrance. Advocates of e-stamp stated that outpayments will induce willingness in consumers to convert to such a model, as their payment account will probably net out or even be positive due to the imbalance of e-mail traffic (they will receive more than they send). They stated that Dutch employers association VNO-NCW endorses a study on the viability of such a payment proposal, as they think it looks promising. A similar position has been taken by the Direct Marketing industry.

- End-users who prefer the introduction of e-stamps should endorse it in public.

7.2 Service providers should shift focus to proxies and sending mail

The Internet Industry, and e-mail service providers in particular, have already taken a range of countermeasures. This section lists them in brief, and elaborates on some new proposals.

7.2.1 Legal actions

Nearly all industry parties in the Netherlands have established general conditions and acceptable use policies for their users that allow them to intervene if a client starts spamming. Enforcement of these policies is relatively easy for senders of spam on an ISP's network. XS4all has sued bulk e-mailer Ab.fab in a high-profile court case, and comparable litigation can be found in other countries. Litigation against spam by ISPs can be performed individually and collectively (assisted by industry associations). Several cases in the Netherlands and the US have been successful.

These private legal means have reached their limits as spam has gone underground with zombie PCs and outgoing sources have often become invisible for ISPs. Therefore influencing policy makers to institute fiercer laws and higher fines is an option, adding a criminal prosecution option for the use of zombie PCs.

- To support legal action and to better assist monitoring and enforcement, ISPs should maintain records and files on events in order to be able to co-operate with investigating or prosecuting authorities and join in litigation cases.

7.2.2 Technological actions

A large number of technological countermeasures have been taken, as is shown by the extensive listing in Chapter 6. Not all ISPs have implemented all of them. Business-oriented ISPs often deliver open Internet connectivity without technical restrictions on protocols, and opinions diverge on what clients require. Some restrictive solutions are therefore controversial. Providers of consumer Internet access and web-based e-mail services have different requirements and pursue different countermeasures.

- ISPs should offer different quality levels of spam tagging, blocking and filtering techniques that can be tailored to the variety in needs of their clients.

Most current efforts for ISPs with access networks are directed toward clamping down on zombie PCs and avoiding the large-scale virus infections that may create them. Several new proposed actions in this area are:

- Installing Sender Policy Framework, registering SPF records in the DNS for outbound e-mail servers and observing its contribution to better detection of spam before including it in filters
- Blocking outgoing e-mail (port 25) and forcing the use of the ISP's mail servers for outbound
- Using authenticated mail from customers and mail servers for sending through the ISP servers
- Establishing monitoring of users requiring open Internet access.

The use of SPF in its current form should not be promoted as the prime anti-spam tool, as SPF allows a straw man to register hit-and-run domain names. We advise it mainly as a means to counter impersonation (spoofing) and in particular to reduce the attractiveness of using zombie PCs. Forcing outgoing mail to pass through ISP platforms is a controversial issue. For some ISPs we recommend they should at least establish a monitoring alternative.

ISPs can perform other activities that are also directed toward technical detection of outgoing bulk e-mail and that can underpin monitoring and enforcement of contracts and general terms of trade on sending bulk e-mail

- ISPs should filter and screen outbound mail on bulk e-mail characteristics, applying bulk limits, PPO (= Prior Permission Only)
- ISPs should assess and apply more efficient ways (timing, routing, etc) to recognise and handle both spam and legitimate e-mail such as lists, newsletters etc.

Practically all ISPs and mail server operators (except spammers) receive more e-mail than they send. For them monitoring outgoing spam is more effective and more efficient than monitoring incoming mail. As an added advantage outgoing spam can be recognised by its traffic characteristics in relation to client-contracts, therefore there is no need to look at the content. This will stop the arms race, and will relieve ISPs from the heavier and unwanted burden of having to monitor the content of e-mails.

Two sets of technological actions can be taken that tackle the root of the problems: focussing on viruses spread by e-mail as the main source of zombie PCs, and investigating the response websites used by spammers

- ISPs could co-operate in feeding and maintaining the virus block list
- ISPs could decide on extending block lists to URLs and spam domains
- ISPs could extend tools that relate spam to domain names and name servers to insert a redirect website that warns users.

Websites deployed by spammers for receiving responses or measuring tracking ".gifs" need to stay up for days instead of seconds (proxies) to hours (mail servers). These sites can be listed in a URL blocklist to be used by a filter that performs time-consuming deep mail inspection. An alternative is to load the specific domain names of the list into the local cache of the ISP's domain name server, redirecting users to an ISP webproxy with a warning and an explanation on how to configure spam filtering.

7.2.3 Behavioural (social and organisational) actions

ISPs can actively support both individual and collective self-regulation regarding the sending of spam. It is imperative that spam is not allowed to be sent from their network. They can co-operate further on feeding blacklists and installing honeypots and honeyproxies to trap spam or assist prosecution. The financial basis of several of the anti-spam activities and abuse lists is still remarkably thin. Several of the most prominent sites are still operating on volunteer work by system administrators.

- ISPs can strengthen collective anti-spam initiatives not only by contributing, but also by 'in kind' gifts to these initiatives (such as hosting blacklist servers and websites)

Commercial efforts are more directed toward developing and selling (physical) anti-spam systems and software and on customising anti-spam systems for firms. Each of these draw at least in part on the volunteered collective systems. This mode of

operation (participating in the effort, while bearing one's own costs) resembles practices frequently encountered in standards organisations and other technical communities. They can be sustained as the interests in contributing and drawing from these common pool efforts are obvious. The stability of this bartering style is a characteristic of many Internet institutions. However, if spam continues to be a problem further commercialisation of these services (shifts to fee basis) are to be expected, as this brings more accountability.

In the same vein, one of the major tasks for ISPs and owners of e-mail servers in general is to raise their users' awareness of spam and to educate them on how to handle spam and how to activate filtering functions.

Most of the interests of ISPs also apply to (web)hosters and fixed and mobile telecommunications operators. Their role differs from ISPs and mail system owners because their profits increase with the amount of traffic. However, we found that the income they derive from carrying spam traffic is too low compared to the damage to the public interest of a properly functioning Internet, trusted by the public. This opens up possibilities for behavioural pressure.

- Web hosters can develop rate-limiting and monitoring systems, refuse to host websites obviously engaged in the business of selling tools for spamming, and supply instructions to customers on how to protect their systems against misuse by spammers.
- Fixed and mobile telecom operators are more limited, as e-mail is in the application area. They can however monitor traffic and assist in tracing sources of spam.
- Major backbone operators can exert social pressure. They can pressurise webhosters linked to their network or located in their data centres not to host websites that are obviously in the business of selling spam software, harvesting tools etc.

7.2.4 Economic actions

- ISPs could alter their contracts to adhere to the adage: Mail is free, bulk is not.

A commercial bulk policy is set to allow all bulk-mail (above a private threshold) to go out by permission only. It can be regulated by different timing (a night batch), speed (half the speed), different routes (where there is room) and subscription / fees (for commercial mail). The contractor is required to guarantee good behaviour, and is responsible under heavy penalty for sending only opt-in bulk.

A more extensive economic approach is to introduce the e-stamp. This is not easily done by a single player. It requires collective action, with the participation of at least some of the largest consumer ISPs in the Netherlands. The failure of adoption of Sender ID by major US ISPs, due to patent and licensing discussions with Microsoft,

has shown that efforts to raise authentication and provide future means for introducing an e-stamp can fail on the specifics of the market structure and a lack of trust in the commercial agenda.

Many in the market doubt the willingness of end-users to start paying and therefore the viability of this approach. A coalition of end users and ISPs who own e-mail domains in the Netherlands are currently discussing the open source "MONS" system, developed by Dutch Internet veteran C. Verhoef for certifying mail servers and introducing an e-stamp, while further development and implementation is studied by TNO Telecom.

The proposal is to add to an e-mail an envelope that labels originator, addressee, message ID and checksums. This envelope allows mail server owners to perform a check on the origin of the mail in a manner resembling SPF, while it adds the option of establishing a central clearing house to net payments and certifying mail server owners as well as sanctioning misbehaviour with termination of the contracts).

In this proposal the economic incentive is established as the end-users are receiving a compensation fee per incoming e-mail, while they pay for sending e-mails. This will mean consumers often end as net beneficiaries. The proposal contains open source development of the envelope labels, but the most important effort is a substantive collective action with participation of major industry parties, at least on a national scale. The cost of the development of the necessary software code for the e-mail system and the clearing house is assumed to run into several hundreds of thousands of Euros. Organising the collective clearing system by bringing parties together writing out the details, promoting it and certifying first users will require a similar financial effort. Its being a collective action makes it a far more difficult and risky effort. The success of its launch on a national scale will depend on the percentage of e-mail sent that is directed to other Dutch people and organisations[52].

History has shown that payment systems can often be successful on a national scale.

- The Dutch Internet Industry should seriously discuss the viability of collectively establishing a national e-stamp system

7.3 Legitimate senders should distinguish themselves from spammers

Legitimate senders of bulk e-mail should distinguish themselves more clearly from spammers. This section lists their actions in brief, and elaborates on some new proposals.

[52] It should be noted that 5 million Dutch citizens use MSN, a service located in the USA. They mainly use MSN for instant messaging, but many also have a Hotmail e-mail account.

7.3.1 Legal actions

Writing and adhering to a code of conduct for sending e-mail by the direct marketing industry has proved difficult. Although this was partly due to the collapse of the DMSA, the ECP.NL-led initiative of 2003 was mentioned as an example by the European Commission, but it ran into problems in discussions with ISPs. The conflict centred on demands of whitelisting of the mail servers of known direct marketers (e.g. members of EMMA-NL). According to end-user advocacy groups some e-mail marketers fail to adhere to the self-regulatory code of conduct. We observe there is a climate of distrust which leads to lengthy negotiations.

However, to this day OPTA has received few complaints about bulk e-mail marketing conducted by a major Dutch firm, the far majority are sent by obscure small enterprises. Comparing views of DDMA and OPTA on the new legislation, there appears to exist a difference in interpretation of the extent of the opt-in clauses for promotional material of third party products and services. Due to a lack of complaints, a restrictive (OPTA) or more lenient (DDMA) explanation is not on the agenda, and jurisprudence may be a number of years in the making.

Ideally, the legitimate senders do not have to do anything other than to adhere to their code of conduct. We would like to point out that the commercial companies are establishing a code of conduct, but organisations sending bulk e-mail with political and charitable ends are not active in this field. However, OPTA has not received a complaint about an unsolicited bulk e-mail belonging to this category either.

7.3.2 Technological actions

On the technological side legitimate senders of bulk e-mail and their ISP (usually EMMA-NL) should take care that bulk-mailings do not put stress on other ISP's systems. A potential measure to guarantee avoiding stress is to add a free header to the e-mail indicating the bulk nature. This enables receiving ISPs to put the mail in a different queue and allow a delay in further processing.

- Legitimate e-mail marketers should take technological measures to avoid stressing systems of mail receivers, for instance by adding headers that allow recognition for low priority scheduling.

7.3.3 Behavioural (social and organisational) actions

In discussions we found that an essential difference between legitimate senders and spammers lies in the way they acquire third party e-mail addresses (a one time rent from a source versus buying a CD with harvested addresses, or performing dictionary attacks on ISP servers). How the address was acquired is unclear for most recipients.

Several behavioural actions can still be taken, despite the fact that complaints about legitimate senders of bulk e-mail have not yet been made. E-mail marketers may put

more effort into establishing guidelines that define the difference between them and illicit senders better to reduce distrust. This is an action that can be taken in collaboration with other actors. It is in their interest to do so, since illicit senders ruin the image of e-mail and the Internet.

In our interview the DDMA proposed a measure . Senders of e-mail marketing should clearly identify the source of the address when renting it from a third party. Most do not. This makes it difficult for recipients to evaluate the undo of an opt-in. This is also the case if they are part of the business community. Such actions, although not required by law, can raise trust in e-mail marketing.

- Finally, associations of e-mail marketing could educate their community and clients better on the scope of the Telecommunications Act. They should point out that the restriction to natural persons in Article 11.8 means that e-mail marketers are not allowed to send unsolicited commercial e-mail to most small firms and free lancers, as they are natural persons and not legal persons under Dutch Law.Legitimate senders should include the source of the e-mail address in their mail.
- Legitimate senders should restrict their unsolicited mail to legal persons only and adhere to the law regarding small businesses that are natural persons.
- Senders should monitor the legitimate character of (mailings by) themselves and colleagues to demonstrate capability of self-regulation and self-restraint

7.3.4 Economic actions

We have been informed that both e-mail marketers and representatives of employers associations are quite positive on proposals to study the viability of a certified central clearinghouse for e-stamps. Therefore facilitating a serious effort to co-operate in establishing and testing such a system would raise credibility.

7.4 The Government should foster initiatives

The Government can stimulate the initiatives for countermeasures and interventions to reduce spam in the ways described above. They do however have an independent role, in particular in the fields of legislation, monitoring and enforcement under the new Act. Now that the Act has come into force, one of the prime roles of the Government is to educate citizens and (not-for-profit) corporations and raise awareness of the new Act.

7.4.1 Legal actions

The largest amount of incoming spam in the Netherlands has its origins in other countries. Citizens and even large corporations are relatively powerless outside their national borders. Governments should speed up law making and international co-ordination to align countermeasures. They could act against non-responsive countries.

As the image of the Internet deters under the current spam load, they could prioritise investigating and prosecuting spammers, both nationally and internationally. Complaints on large international unsolicited bulk e-mail runs from a Dutch source could have a lasting detrimental effect on cross-border collaboration.

One other legal action, proven successful in at least one other European country, is levelling the privacy-playing field between mail senders and recipient. Consumers now already have the right (Privacy Law) to demand the origin of their email-address, and to have their data corrected and deleted, if they so wish. To effect that right however they have to go through lengthy, user-unfriendly and "paper/letter" procedures. Again placing time and money burdens on recipients.
Senders of commercial e-mail should be obliged to make the opt-out and the inform/correct/delete options for consumers as easy and cheap (i.e. by simply sending an e-mail) as the intrusion itself.

7.4.2 Technological actions

Governments can fund research into improving the actions described above. Many initiatives are underfunded due to their volunteer character and collective action characteristics. Spam enforcers can trace sources of spam and destinations of responses. Currently enforcers are geared to tracing the persons behind a destination, often by determining who maintains and owns the website. This increases the effort submitters of spam need to put into hiding the trace to the source with relaying and proxies. Honeypots and honeyproxies logging attempts to send spam are used to cast a net. They can be a source of evidence for enforcement authorities, who may choose to collaborate with honeypot and honeyproxy maintainers in advance. Authorities could also finance projects to install and maintain honeypots and honeyproxies.

7.4.3 Behavioural (social and organisational) actions

Besides its task of raising awareness and educating the people, the Government can set an example and initiate and host meetings between relevant actors (like the current activities of the Justice Department with regard to N&TD[53]).

Some of the proposed collective actions are mistrusted by (groups of) actors when others dominate the initiative. Such initiatives tend to get a negotiation character and see an early demise. To avoid this the Government can choose to steward the talks and stimulate actors to make progress.

7.4.4 Economic actions

One of the most complex initiatives is to co-ordinate the initiative for an e-stamp. This approach has been proposed several times, but the fragmented market has not been able

[53] A Notice and Take Down procedure is discussed for illegal content

to establish it. For start-ups the ubiquitous nature of e-mail poses difficulties in establishing a solution, as the co-ordination effort requires too many resources for them.

Clearly an attempt to introduce a payment system has a system-wide impact. Radically changing the economics of mail is not unique in history. The introduction of the prepaid stamp in 1830 in England was a similar effort to change the economics of a 'recipient pays' system[54] to a 'sender pays' system.

- The Government should stimulate talks on an open payment system trial
- The Government could act as a launching customer to give the open payment system trial a serious chance.

[54] The prepaid postage stamp was introduced in 1830. Before then recipients paid by weight. The system was changed after people started sending bricks to those they disliked. See A.M. Odlyzko, The history of Communications

8 Conclusions and a proposal for allocating responsibilities and assigning authority

In this chapter we will draw some general conclusions and formulate proposals for allocating responsibilities and assigning authority to bodies or groups to act in concert on the various intervention points that the business case for spam offers. Concerted effort against the acts of a limited group of rogue entrepreneurs who flood the global mail system with spam has the consequence that interests of various groups must be balanced to align everyone. Otherwise various actors may spend more time in fighting each other than fighting spam. The first section provides conclusions, the next discusses the balancing act, the third section discusses allocating responsibilities and the last section discusses proposals for assigning authority

8.1 Conclusions

Fighting spam is a daunting task as it is most effectively executed only when the many actors involved operate in concert. Spam creates a negative image for the large majority of Internet users who do not want to engage in a transaction with a spam source. They spend time on removing the unsolicited mail and bear the costs in receiving it through metered dial up. Spam diminishes the reputation of e-mail and the Internet as a reliable and trusted venue for information exchange and transactions. The size of these negative external effects justifies interventions.

Based on data we gathered in interviews and fact checking, covering 5% of Dutch mailboxes, we conclude that ca. 145 million spam messages arrive per day at Dutch mail servers, constituting 75% of the total incoming e-mail. This flood of spam to 10 million Dutch mailboxes costs our society € 116 million per year. The majority of these costs is productivity loss, due to the need to determine and click away spam and higher dial up charges for downloading spam to the PC. Spam would have cost Dutch society € 1.7 billion per year, when ISPs and mail owners had not already installed anti-spam techniques for ca. € 16 million.
The senders of spam are not confronted with these cost. To maintain a daily bombardment of 145 million unsolicited messages on the Netherlands, they have to pay up to € 4 million per year on current market rates for hiring capacity on Zombie PC's. This amount has to be justified by their business case.

We analysed the business case of a sender of spam, to find potential intervention points. We concluded a sender of spam needs at least five inputs: a spam program, control over a lost of proxies (ZombiePC's) or access to mail relays, a list of e-mail addresses or a harvesting program, network access at substantive capacity and “Bulletproof” webhosting. A potential sixth input is a link to a financial payment system to complete the transaction proposed with the spam. These inputs determine the

cost to reach out to recipients. The number of recipients who do not filter or discard the spam and instead read the unsolicited bulk e-mail and respond to it (via the bulletproof website) and become a customer are determining the total acquisition cost per customer, which in turn determines the needed margin on products offered. Countermeasures can be just intervene at the end.

Actors confronted with spam have already introduced a growing number of countermeasures in the past years. We have described current technological, behavioural and legal countermeasures in chapter 6 and found that the nature of economic countermeasures today is quite indirect. The impact of recently introduced anti-spam legislation on the behaviour of Dutch spam sources cannot yet be assessed in full, as the first administrative fines procedures of OPTA are planned to be completed just before the end of 2004. Legislation seems to have discouraged some spammers, as the number of spamruns from Dutch sources to Dutch users has more than halved this year to less than two spamruns a day on average.

With a potential decline in national spamruns the problem is not yet fixed. More than 99% of the daily volume of spam arriving in Dutch mailboxes stems from foreign sources. This means international collaboration is needed. This is still in its infancy on the side of enforcement. Spam senders also deploy new circumvention techniques like proxies installed on zombie PCs. Where the Dutch broadband users have acted as a major source of spam in the first months of 2004, producing . In the latest country comparisons the Netherlands have fallen out of the Top-25 and is the source

Clearly it is not easy to undermine the business case for spam , as there still are many ways to send large volumes cheaply. In chapter 7 we listed a set of additional intervention points that could be pursued by various actors to further counter the negative effects of spam on society. Several proposals require a high level of collaboration and co-ordination between actors who have different interests.

8.2 Finding the balance to reach parallel goals

With the extension of the legal framework to cover spam, the investigation and enforcement task has been placed on OPTA. For natural persons a shift in balance has occurred in official complaints. One consequence has been the recent announcement of the Board of the Spamvrij Foundation to terminate the foundation. The volunteer community initiative was unique in Europe (they had no counterparts in other countries), but it was not able to bear a growing burden of requests for interviews and informational and educational presentations. As these volunteer efforts are now reduced, raising awareness, informing the people, organisations and the business community about spam and the finer details of the Telecommunications Act will thus become a more important task for the government and for OPTA.

Several persons we interviewed made remarks about the difficulties in self-regulation encountered last year when it proved difficult to align parties behind a Code of Conduct for e-mail marketing. Three organisations, the DDMA, EMMA-NL and the Internet Advertising Bureau NL, came up with different proposals. Discussions became heated when representatives of the ISP association NLIP did not agree with the demands from the e-mail marketers. This debate has now moved to the employers association which is attempting to balance the interests for unsolicited commercial e-mail sent to businesses (legal persons), which was kept in the opt-out regime through heavy political lobbying. In business practices home country law of the supplier is the legal and contractual starting point, while in consumer and privacy areas the laws of the recipient's country prevails. According to several interviewees even in this business-oriented setting finding the balance for a code of conduct between various interests of Direct Marketers, ISPs, e-retailers and multinational firms proves difficult. Aside from this inter industry negotiation, the Dutch privacy authority CBP, employers association VNO-NCW and the largest labour union FNV, have developed a policy code for employees private use of their corporate mailbox.

Our interviews and fact-checking with ISPs and companies responsible for more than 5% of all Dutch mailboxes have shown that filtering spam costs large-scale mail server operations € 1 per year. This is in line with price ranges[55] Brightmail (now Symantec) announced in an interview in 2002. Based on this the global price tag for spending on anti-spam tools and services rises to hundreds of millions. The Dutch market is limited with its current expenditure of € 16 million in a year.
The market has been quite able to come up with technical countermeasures and innovations in the business of spam-filtering and sell them to customers. But they sell stopgaps at the back of the pipeline to block, tag or filter 75% of all incoming e-mail messages in the Netherlands. Replacing the focus to outbound spam and trying to remove the roots of the business case seems more rewarding.

We interviewed several companies with new ideas and proposals. One such proposal concerns a variety of advanced filtering techniques, and already a clear customer (an ISP) is willing to pay. The two other were initiatives, one directed at opt-in mailing lists, the other proposing to introduce *e-stamps*. Both partially rely on collective action and co-operation to reach a broader systemic change. Such efforts require critical mass and a balancing of interests of stakeholders. They are therefore difficult to establish in a venture capital driven start-up setting (the customer is difficult to identify, as it is a collective). The viability of such initiatives can be brought in a broader forum with potential interested stakeholders.

[55] Brightmail announced pricetags of US$ 1-2 and US$ 5- 15 per mailbox per year for ISPs and companies resp. http://www.smallbusinesscomputing.com/webmaster/article.php/1467881

8.3 Allocating responsibilities

We find that not all potential points are currently covered when we compare the list of current countermeasures derived from several new proposals from our interviews and the gaps we found by categorising both in the framework for the toolkit to the potential intervention points that damages the business case for senders of spam.

We have found the following potential intervention points to damage the business case of spammers:

- Purchasing a spam program
- Control over (a list of) proxies or access to mail relays or servers
- Buying or harvesting e-mail addresses
- Network access
- Bulletproof webhosting
- The financial payment system
- The cost of reaching out to recipients
- 'Willingness to buy' of a recipient
- Skills to release Zombie-PC viruses

Most technical countermeasures and the prohibitions and clauses in legislation are effectively concerned with deterring senders in general, reducing their lucrative business case by limiting the number of recipients reached by spam, and requiring authentication of the senders. Several of these are mere stopgaps to dam the incoming spam flood. They influence the business case by indirect means as they partially reduce the reach of spam or the response rate and thus raise the cost to reach out.

A number of countermeasures are oriented towards denying senders of spam to get network access, some are oriented towards limiting their access to proxies, mail relays and mail servers. Many educating and awareness raising efforts to inform end-users not to respond to spam and hand out their e-mail address with care tend to make address acquisition less easy and more costly. Most technical measures and the prohibitions and clauses in legislation are also oriented towards limiting the number of recipients and requiring authentication of the senders.

Most proposals however still attempt to raise the cost for spammers by non-economic means. One proposal attempts to address the economic problem. The external cost imposed on the recipient is not internalised in the system and is not signalled back to the sender in the form of a fee. This route can take several forms, one of them being called *e-stamp*, and has not yet been tried, but it is presently at the heart of discussing the business case. An e-stamp of a few Eurocents destroys the business cases of senders of spam by a thousand-fold increase in their cost .

Also few countermeasures address potential intervention points in the business case such as the commercial availability of spam programs, the way e-mail addresses are acquired, bulletproof webhosting and the link to financial payment systems required by spammers to complete the transaction.

In chapter 7 we provided detailed lists with countermeasures that could be taken or expanded per actor or group of stakeholders. Most responsibilities of actors have been clearly identified. This is however less obvious for some proposals where collective actions are needed to align parties.

Below we summarise per actor what we consider the most recommended actions and indicate where responsibility can be allocated by the various actors and stakeholders.

1. End-users should know how to behave with regard to spam and take preventive measures (the Government, Internet industry, consumer-organisations and employers can assist with an information campaign)[56]
2. The Internet industry should implement measures on all levels (hardware, software and network) against spam distributed through proxies (zombie PCs), like authenticating mail servers, and support collective anti-spam initiatives.
3. The Internet industry ISPs filter and screen outbound mail on bulk e-mail characteristics, applying bulk limits, PPO (= Prior Permission Only)
4. Legitimate senders should show the origin of the address (list?) used to send the e-mail, to facilitate de-listing from the original list.
5. The government and OPTA should explain the extent of the Telecommunications Act to the public, and in particular to the (small) business community, in far more detail[57].
6. The government should convene representatives of all actors to establish a serious study on the viability of voluntary and multi-party (self-regulation-) approaches to implement sender pays mechanisms.
7. A similar initiative should be taken at the EU-level, with at least FEDMA, Euro-ISPA, BEUC, the ERG and EDPS represented.
8. The government should focus Dutch efforts on outbound spam, and the use of (viruses to create) open proxies and engage in international co-ordination for inbound spam.
9. The government should study present and future legal options to intervene at points in the business case not yet explored in current countermeasures, such as the sale of spam programs, the trade in access time to proxies, the link to a financial payment system, bulletproof webhosting and the manner in which address lists are acquired.

8.4 Assigning authority

Most initiatives and recommendations we list in the section above are directed at diminishing the business case for spam. As laws have been written, anti-spam activities

[56] See http://www.aca.gov.au/consumer_info/spam/informationforbusiness.htm as an example.
[57] The restriction in article 11.8 to *natural persons*, a category that includes many small businesses, is not easy understood legalese for a layman. Small businesses are not familiar with their rights to complain about Spam at OPTA etc. Marketers think they are allowed to send mail to anyone that operates a business.

are more formalised and self-regulation is reduced. In this section we discuss two areas where the criminal boundaries are touched and authority is best assigned to the law enforcement area and not to self-regulatory bodies.
In several cases spam is used to market goods and services that are illegal in a number of countries, or have purposefully been made difficult to obtain (e.g. prescription drugs). Tracing people who offer these goods is the field of criminal investigation, as they frequently tend to start to misbehave and threaten people who confront them.

We learned that very few formal complaints at OPTA concern acts of high profile firms and they have not received any complaint about spam promoting political and charitable ends. The shady business characteristics of the senders of spam are now obvious. In all of OPTA's anti-spam-teams, as described in chapter 4, a member of the national *Digitale Recherche* is present. This covers the potential for criminal investigation and prosecution. Two remarks are made in this section on assigning authority to law enforcement that goes one step further than the current anti-spam practice.

An interviewed ISP suggests that the current procedure and organisation of the Dutch police forces is not quite suited for reporting a Denial of Service attack implemented by a spam-bomb. ISPs are currently required to report such incidents for criminal investigation at local police stations, which lack the skilled staff to understand the problems. The situation would improve if such Denial of Service attacks could be reported to some central specialist group linked to the national *Digitale Recherche* or the High Tech Crime Centre recently established and started. This has the not-to-underestimate advantage that experiences and synergies from combating other types of cyber-abuse (illegal content, illegal activities, etc) can be used.

International hard core spammers have not only pumped up the sheer volume of their unsolicited bulk mail to get their message through; they also deploy new circumventing methods. Nearly all spamruns are now relayed through proxies that are often installed by means of viruses or spyware on broadband end-users' PCs. This phenomenon makes the Netherlands, with its high number of broadband users, vulnerable to acting as a spam relay. The industry can establish a package of anti-zombie PC measures and set up systems to detect proxy scans, for instance by installing honeyproxies that reveal the source (IP-address) of the proxy-scanner. Such efforts might be established in close collaboration with law enforcement task forces that can present the logs of honeyproxies as evidence in Court.

We thus recommend the government to improve the means for ISPs to report a major attack on their systems and to co-ordinate with ISPs the establishment of honeyproxies, whose log files can be used in prosecution. Authority can be best assigned to cyber crime law enforcement forces in these cases.

Annex A Dutch Law relating to spam

This Annex contains the Dutch text of relevant Telecommunications Act's articles.

Telecommunicatiewet

Artikel 11.7
1. Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is uitsluitend toegestaan, indien de desbetreffende abonnee daarvoor voorafgaand toestemming heeft verleend, onverminderd hetgeen is bepaald in het tweede lid.
2. Een ieder die elektronische contactgegevens voor elektronische berichten heeft verkregen in het kader van de verkoop van zijn product of dienst mag deze gegevens gebruiken voor het overbrengen van communicatie voor commerciële doeleinden met betrekking tot eigen gelijksoortige producten of diensten, mits bij de verkrijging van de contactgegevens aan de klant duidelijk en uitdrukkelijk de gelegenheid is geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens, en, indien de klant hiervan geen gebruik heeft gemaakt, hem bij elke overgebrachte communicatie de mogelijkheid wordt geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Artikel 41, tweede lid, van de Wet bescherming persoonsgegevens is van overeenkomstige toepassing.
3. Bij het gebruik van elektronische berichten voor de in het eerste lid genoemde doeleinden dienen te allen tijde de volgende gegevens te worden vermeld:
a. de werkelijke identiteit van degene namens wie de communicatie wordt overgebracht, en
b. een geldig postadres of nummer waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten.
4. Het gebruik van andere dan de in het eerste lid bedoelde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is toegestaan, tenzij de desbetreffende abonnee te kennen heeft gegeven dat hij communicatie waarbij van deze middelen gebruik wordt gemaakt, niet wenst te ontvangen. Aan de abonnee worden in dat geval geen kosten in rekening gebracht van voorzieningen waarmee wordt voorkomen dat hem een ongevraagde communicatie wordt overgebracht.
5. Degene die ongevraagd communicatie voor commerciële, ideële of charitatieve doeleinden overbrengt, neemt passende maatregelen om ten minste eenmaal per jaar de betrokkenen bekend te maken met de mogelijkheid tot het doen van een kennisgeving als bedoeld in het vierde lid. De bekendmaking kan via een of meer dag-, nieuws- of huis-aan-huisbladen of op een andere geschikte wijze plaatsvinden.
Artikel 11.8

De toepassing van de artikelen 11.6 en 11.7 is beperkt tot abonnees die natuurlijke personen zijn.

MEMORIE VAN TOELICHTING

1. Motivering van het wetsvoorstel

e. Richtlijn 2002/58/EG van het Europees Parlement en de Raad van de Europese Unie inzake de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie, verder: richtlijn nr. 2002/58/EG) (PbEG L201),

8.4 Ongevraagde communicatie

Evenals in richtlijn nr. 97/66/EG geeft richtlijn nr. 2002/58/EG een regeling voor ongevraagde communicatie ten behoeve van direct marketingdoeleinden. In beide richtlijnen is het gebruik van automatische oproepautomaten zonder menselijke tussenkomst en faxen voor het overbrengen van ongevraagde communicatie (in richtlijn nr. 97/66/EG: het doen van ongevraagde oproepen) voor direct marketingdoeleinden onderworpen aan voorafgaande toestemming van de abonnee; dit wordt ook wel aangeduid als het opt-in regime. Richtlijn nr. 2002/58/EG geeft hieraan een belangrijke uitbreiding door ook het gebruik van «e-mail» (elektronische berichten) voor het overbrengen van ongevraagde communicatie voor direct marketingdoeleinden – zoals gedefinieerd in artikel 2 van de richtlijn en omgezet in artikel 11.1 van dit wetsvoorstel – onder de werking van het opt-in regime te brengen. Het gaat dan niet alleen om elektronische post (e-mail in enge zin), maar bijvoorbeeld ook om het gebruik van SMS en MMS. Reden om ook deze middelen onder het opt-in regime te brengen is dat deze middelen door degene die zich hiervan bedient op vrij eenvoudige wijze en goedkoop kunnen worden ingezet, terwijl de lasten – in de brede zin van het woord – waar het gaat om de verzending van e-mail in de enge zin van het woord (exclusief SMS) vrijwel volledig komen te liggen bij de aanbieders van openbare elektronische communicatienetwerken en -diensten alsmede de ontvangers van de e-mail. Voor de ontvangers treden er kosten op als gevolg van het downloaden van e-mail; overigens nemen deze kosten af, indien men gebruik maakt van flat fee internet. Daarnaast moet ook niet de ergernis bij de ontvanger worden vergeten, in de gevallen dat deze regelmatig met grote hoeveelheden ongevraagde e-mail of SMS wordt bestookt («spam»). Een andere belangrijke reden vormt het feit dat bij het verzenden van dergelijke e-mail (in enge zin) de kosten van transport eenzijdig worden gelegd bij de aanbieders van elektronische communicatienetwerken en -diensten, die immers de verzonden e-mail bij de ontvangers moeten bezorgen en zolang de mail niet is opgehaald deze moeten bewaren. Al naar gelang de omvang waarin van dit middel gebruik gemaakt wordt, vergt dit investeringen – onder meer in opslagapparatuur – van de desbetreffende aanbieders. Voorts kan de verzending van grote hoeveelheden ongevraagde e-mail tot congestieverschijnselen op het Internet of in de systemen van de desbetreffende aanbieders leiden. Op de

hoofdregel van opt-in voor het gebruik van elektronische berichten, wordt in de richtlijn een uitzondering gemaakt waar het gaat om het gebruik van elektronische contactgegevens voor e-mail die men in het kader van de verkoop van een product of dienst heeft verkregen. In dergelijke gevallen geldt een opt-out regime (men kan tegen het gebruik ervan verzet aantekenen). Op de mogelijkheid tot het doen van verzet moet de klant echter nadrukkelijk bij de verzameling van de bedoelde contactgegevens worden gewezen; en vervolgens bij elk gebruik dat ervan gemaakt wordt.

In richtlijn nr. 2002/58/EG worden vervolgens met betrekking tot het gebruik van e-mail voor het doen van ongevraagde oproepen als hier bedoeld, vervolgens nog enkele aanvullende eisen gesteld. Het gebruik van andere middelen dan automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie ten behoeve van direct marketingdoeleinden zal onderworpen blijven aan het zogeheten opt-out regime. Dat betekent dat het gebruik van dergelijke middelen is toegestaan, tenzij de abonnee te kennen heeft gegeven dat hij communicatie waarbij van deze middelen gebruik wordt gemaakt, niet wenst te ontvangen.

Onderdeel Av (vervangen artikel 11.7)
Artikel 13 van de nieuwe privacyrichtlijn voor elektronische communicatie geeft een regeling voor ongewenste[24] communicatie met het oog op direct marketing. Deze regeling volgt in hoofdlijnen het stramien van artikel 12 van richtlijn nr. 97/66/EG, zij het dat met name waar het gaat om het gebruik van elektronische berichten voor direct marketingdoeleinden er een specifiek regime wordt geïntroduceerd. Het voorgestelde artikel 11.7 strekt ter vervanging van het huidige artikel 11.7, waarin artikel 12 van richtlijn nr. 97/66/EG is geïmplementeerd.
In artikel 13 van de nieuwe privacyrichtlijn wordt – anders dan in artikel 12 van richtlijn nr. 97/66/EG – het gebruik van elektronische berichten voor direct marketing doeleinden onder het zogeheten opt-in regime gebracht. Dat betekent dat – evenals al het geval was voor het gebruik van automatische oproepsystemen zonder menselijke tussenkomst[25] en faxen voor dit doel – het gebruik van elektronische berichten slechts is toegestaan indien de desbetreffende abonnee daarvoor voorafgaand toestemming heeft verleend. De begrippen elektronisch bericht en toestemming zijn in artikel 11.1 gedefinieerd; verwezen wordt naar de daarop betrekking hebbende artikelsgewijze toelichting. Voor de invulling van het begrip «direct marketing» wordt de bij de implementatie van artikel 12 van richtlijn nr. 97/66/EG daaraan gegeven invulling gehandhaafd. In artikel 11.7, eerste lid, wordt dan ook gesproken over het gebruik van de hier bedoelde systemen voor commerciële, ideële en charitatieve doeleinden. Voor de daaraan ten grondslag liggende redenen wordt kortheidshalve verwezen naar hetgeen indertijd bij de parlementaire behandeling is gewisseld[26]. In artikel 11.7, tweede lid, is een specifieke voorziening getroffen voor het gebruik van zogeheten elektronische contactgegevens voor elektronische berichten die men in het kader van een bestaande klantrela

tie, namelijk bij de verkoop van een product of dienst, heeft verworven. Onder elektronische contactgegevens moet in dit verband niet alleen worden verstaan het adres voor elektronische post, maar ook het mobiele telefoonnummer, indien dat gebruikt wordt voor de verzending van SMS- of MMS-berichten voor commerciële doeleinden. Anders dan in het eerste lid, is de reikwijdte van het tweede lid beperkt tot het gebruik van e-mail voor commerciële doeleinden. Gelet op de formulering van artikel 13, tweede lid, van de nieuwe privacyrichtlijn en de daarop betrekking hebbende overweging 41, is deze interpretatie gerechtvaardigd. Het gebruik van langs deze weg verkregen elektronische contactgegevens is daarbij gebonden aan enkele voorwaarden. Allereerst dient de klant bij de verzameling van de contactgegevens duidelijk en uitdrukkelijk de gelegenheid te worden geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van deze contactgegevens. Indien de klant bij deze gelegenheid geen verzet heeft aangetekend, moet hem echter bij elke overgebrachte communicatie de mogelijkheid worden geboden om onder dezelfde voorwaarden – te weten kosteloos en op gemakkelijke wijze – verzet aan te tekenen tegen het verder gebruik dat van zijn contactgegevens wordt gemaakt voor dit doel. Artikel 41, tweede lid, van de Wet bescherming persoonsgegevens is hierbij van overeenkomstige toepassing verklaard; dat wil zeggen dat degene die de contactgegevens voor het hier bedoelde doel heeft aangewend, maatregelen dient te nemen om in het geval van verzet de verwerking van deze gegevens voor dat doel terstond te beëindigen.
Aan het gebruik van elektronische berichten voor de toezending van ongevraagde communicatie voor de in het eerste en tweede lid bedoelde doeleinden wordt voorts in het derde lid nog een aanvullende eis gesteld. Bij het gebruik van elektronische berichten voor deze doeleinden dient te allen tijde de werkelijke identiteit van degene namens wie de communicatie wordt overgebracht te worden vermeld (het gebruik van een pseudoniem is derhalve niet toegestaan); voorts dient in het elektronisch bericht een geldig postadres of nummer[27] te worden vermeld waar de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan indienen. Het niet voldoen aan deze eis wordt als economisch delict strafbaar gesteld.
Artikel 11.7, vierde en vijfde lid, komen overeen met het huidige artikel 11.7, tweede en derde lid, met dien verstande dat daarin enkele begripsmatige wijzigingen zijn aangebracht. Het gebruik van andere dan de in het eerste lid van artikel 11.7 genoemde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden is onderworpen aan het zogeheten opt-out regime. Van deze andere middelen mag men gebruik maken, tenzij de desbetreffende abonnee daartegen bezwaar heeft gemaakt.

Artikel IV
Dit artikel bevat een aantal aanpassingen van het Burgerlijk Wetboek. In artikel 11.7 Tw zijn voorschriften opgenomen met betrekking tot het overbrengen van ongevraagde communicatie voor direct marketingdoeleinden. Daarbij is het overbrengen van der

gelijke communicatie door middel van elektronische berichten – overeenkomstig het bepaalde in artikel 13 van richtlijn nr. 2002/58/EG – onder de werking van het opt-in regime gebracht. Dat betekent dat voor het langs deze weg overbrengen van ongevraagde communicatie voorafgaande toestemming van de abonnee is vereist. In artikel 46h van Boek 7 van het Burgerlijk Wetboek wordt – in overeenstemming met richtlijn nr. 97/7/EG inzake op afstand gesloten overeenkomsten (PbEG L 144) – een regeling getroffen voor het doen van ongevraagde oproepen ter bevordering van een koop op Tweede Kamer, vergaderjaar 2002–2003, 28 851, nr. 3 178 afstand (direct marketing). Dergelijke oproepen zijn te brengen onder de noemer van ongevraagde communicatie voor commerciële doeleinden als bedoeld in artikel 11.7 Tw. Voorts zullen abonnees - natuurlijke personen (zie artikel 11.8 Tw) vaak als consument (artikel 7:46h BW) worden benaderd voor direct marketingdoeleinden. In het huidige artikel 7:46h BW is hetzelfde regime neergelegd als in het huidige artikel 11.7 Tw, te weten een opt-in regime bij het gebruik van automatische oproepsystemen zonder menselijke tussenkomst en faxen; voor de rest – dus ook elektronische berichten – geldt opt-out. Gelet op de voorgestelde wijziging van artikel 11.7 Tw zou zonder een aanpassing van artikel 7:46h BW de situatie ontstaan, dat het gebruik van elektronische berichten voor het doen van ongevraagde communicatie voor direct marketing doeleinden aan consumentenabonnees onder twee tegenstrijdige regimes (opt-in onderscheidenlijk opt-out) zou komen te vallen. Daarbij komt nog het volgende. In de gevallen dat een consument niet abonnee is, maar bijvoorbeeld de huisgenoot van een abonnee, zou dit meebrengen dat voor de consument niet-abonnee het opt-out regime zou gelden en voor de consumentabonnee het opt-in regime. Het is evident dat dit resultaat niet aanvaardbaar is. Met de voorgestelde wijziging van artikel 7:46h BW wordt deze dan ook in overeenstemming gebracht met het bepaalde in het (nieuwe) artikel 11.7 Tw, dat wil zeggen dat ook bij koop op afstand het gebruik van elektronische berichten onder het opt-in regime wordt gebracht. De mogelijkheid hiertoe bestaat op grond van artikel 14 van richtlijn nr. 97/7/EG (minimumclausule) en artikel 10 van richtlijn 2002/65/EG, waarbij aan de lidstaten een keuzemogelijkheid wordt gelaten tussen opt-in en opt-out. Laatstgenoemde richtlijn is de richtlijn betreffende de verkoop op afstand van financiele diensten aan consumenten (PbEG L 271); daarin is aan de lidstaten eveneens de keuze gelaten of (onder andere) e-mail onder het opt-in dan wel het opt-out regime wordt gebracht. Wat de begrippen «communicatie» en «elektronisch bericht» betreft, wordt verwezen naar hetgeen daaromtrent in de toelichting op artikel 11.1 Tw is gesteld.

Artikelen V tot en met VII

Deze artikelen bevatten aanpassingen van het Wetboek van Strafvordering, de Wet op de inlichtingen- en veiligheidsdiensten 2002 en de Wet op de economische delicten aan de voorgestelde wijzigingen van de Telecommunicatiewet. De aanpassingen zijn – met uitzondering van een hieronder nader toegelichte aanvulling van artikel 1, onder 2°, van de Wet op de economische delicten – uitsluitend wetstechnisch van aard. Inhoude

lijke wijzigingen, voor zover deze niet rechtstreeks voortkomen uit de wetstechnische aanpassingen, zijn niet beoogd. In artikel 1, onder 2°, van de Wet op de economische delicten is artikel 11.7, derde lid, van de Telecommunicatiewet toegevoegd. Artikel 11.7, derde lid, houdt een verbod in om e-mail te gebruiken voor de overbrenging van ongevraagde communicatie voor commerciële, ideële en charitatieve doeleinden, indien de identiteit van degene namens wie de communicatie wordt overgebracht ontbreekt dan wel daarvoor gebruik is gemaakt van een pseudoniem en er geen geldig adres of nummer is vermeld waar de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan indienen.

Annex B A comparison with Direct Marketing

In our interview with the Dutch Dialogue Marketing Association (DDMA) we extensively analysed the value chain of postal mail direct marketing, e-mail marketing to compare it with the chain for spam.

Addressing is the first most important difference between DM en *broadcast* advertisement, the second one is response. What can make or break a business case for DM is having access to a good quality address list, and offering an adequate response channel.

Three key points turn up when comparing the business model for e-mail marketing with that of direct postal mail:

1. The response to electronic mailings appears to be high. The DDMA indicates 30 to 40%. The number of contacts opening newsletters regularly is 90%. The corporate users we interviewed confirmed these statements. They also observed a higher response to their e-mail activities than to postal mail.
2. E-mail marketing can be traced better. Standard features on delivery and mail reading can be activated, and graphics can be inserted in html-pages that load from a website. This informs the sender about the number of readers.
3. E-mail marketing is more divisible, schedulable and adaptable to market segments (different headers for different groups) than printed direct mail.

Spammers differ from e-mail marketers by the related phenomena of (lack of) quality of their address list and low response rate. The other two features, highly appreciated by e-mail marketers as an advantage above postal mail, are also available to spammers. They use for instance the ability to trace to validate their addresses and they are able too to divide, schedule and adapt their spamruns.

The Dutch market size for Direct Marketing (DM) is not fully fixed, as definitions of its extent differ. The DDMA estimates its size between € 10 and € 20 billion.
The Dutch market for classic advertisement (print, radio & TV, Internet banners etc.) is more visible, but is much smaller at € 4.5 billion per year. The tilting of marketing towards DM from classic advertisement is an established trend and is also seen in other countries.

The business case for e-mail as a marketing tool is best compared to its cousin, postal mail. The average cost in the Netherlands for a direct mail in a postal mail package is approx. € 1.08. Typically 5% of the recipients reply, which means a marketer effectively spends approx. € 20 to get into contact with a potential customer, member

or donor. If 25% of these contacts convert into a deal the marketer will have spent € 80 in customer acquisition costs.

Using the cost figures found in the former chapter we can determine the business case for e-mail marketing at a more aggregate level. A total campaign cost of € 15 to € 30 thousand for 10,000 to 150,000 addressees means a cost of € 0.20 to € 1.50 per e-mail. With responses at 30 to 40% the cost of reaching a potential customer, member or donor falls within the range of € 3.75 (mailing of 10,000, 40% response) to € 0,67 (mailing 150,000, 30% response) . At conversion rates of 25%, customer acquisition costs fall to the € 2.70 to € 15 range, enabling a large number of cheaper transactions.

By comparison, sales agents selling a product like broadband Internet access door to door typically receive € 40 per deal. Comparable commissions are paid to street corner teams for acquiring charity donors or selling trial newspaper subscriptions.

A spammer who pays approx.. € 200 to send spam to a relatively recent database of 1 million addresses and who has a response rate of 0.025% (1 for every 4000) and a conversion rate of 25% will incur customer acquisition costs of € 3.20. These rates do not permit marketing of groceries, but they are viable for some otherwise unmarketable goods. A look at the products that are sold through spam clearly shows that the size of the transactions is much higher. This indicates that response rates on spam have fallen from one per thousand to one per ten thousand or even lower, due to spam filtering techniques and user awareness of the nature of the messages. But these growing acquisition cost do not break the business case for spam for these products. The growing customer acquisition cost however might induce hard core spammers to shift more and more into shady areas, illegal trade, fraud and other high margin goods. Observing the goods offered and in particular the recent rise of identity theft and fraud (phishing) it indicates that the business case of spam for regular products is evaporating.

Legitimate senders of bulk e-mail incur campaign costs that rapidly rise above € 0.20 per e-mail, depending on campaign size and the specificity of the e-mail address rented (where prices vary between € 0.04 - € 0.40 per address). The DDMA estimates the total spending of their sector on e-mail marketing in the Netherlands at € 100 - € 125 million per year.

When we calculated the direct cost incurred by hard core spammers to send their 145 million mails per day to Dutch receivers we end up at a cost level of ca. US$ 15,000 per day or € 4 million per year. This demonstrates that in financial size spam has a considerable cost. It suggests that hard core spammers must be able to realise a turnover of more than € 10 million per year on the Dutch market.

These advantages over postal mail clearly demonstrate that the business case for e-mail marketing for a range of products of regular companies will continue to exist even if the costs amount to a level above € 1 per e-mail, instead of the current € 0,10. From the points listed above it becomes clear why in some cases the DM sector, is willing to pay up to € 0.50 per direct e-mail, as they told an initiator of an anti-spam e-mail payment schedule.

Annex C Toolkit scheme linked to paragraphs

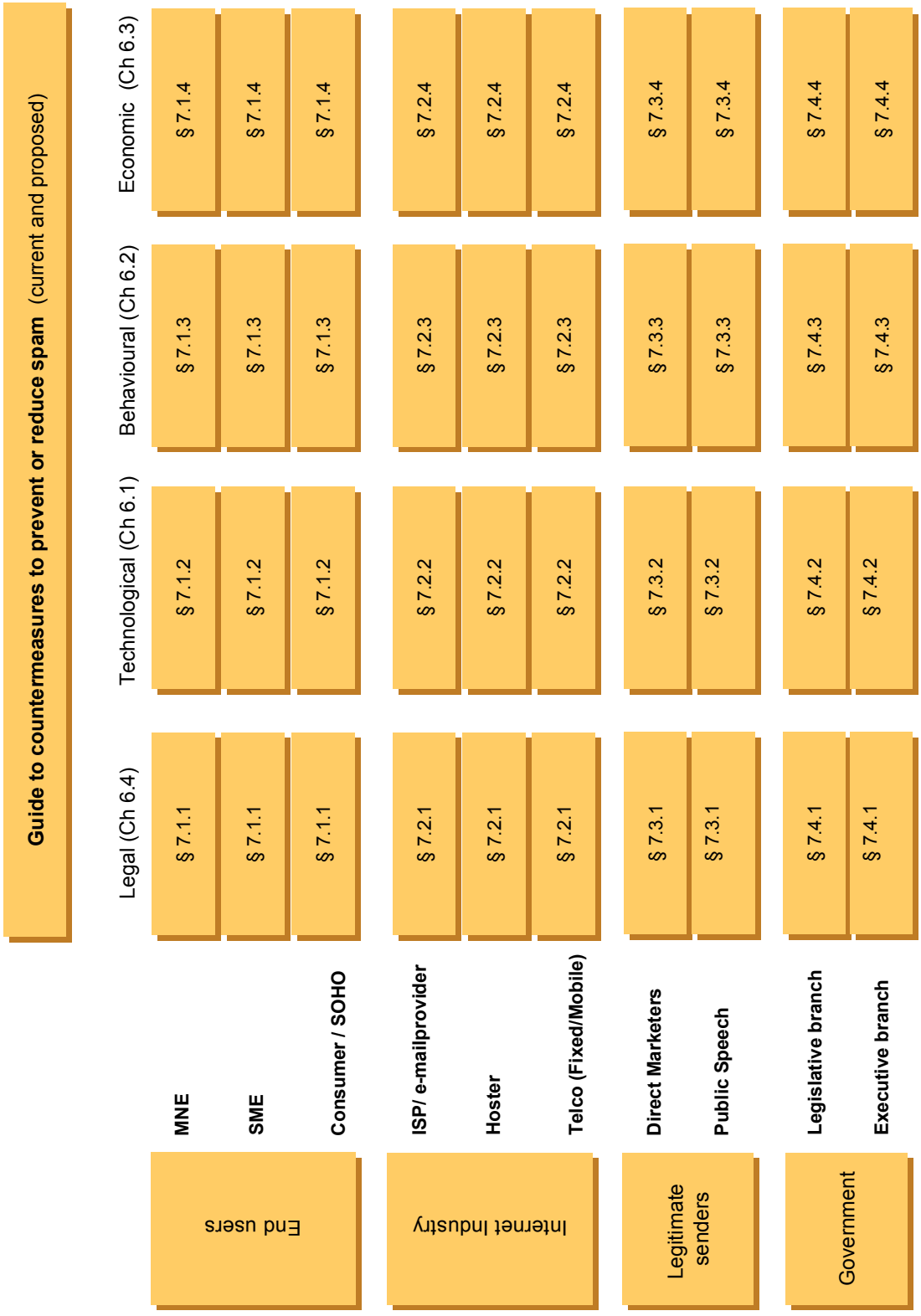


Figure C-1 *Guide to Toolkit with countermeasures that can be taken by various actors*