Ministerie van Justitie

Platform Interceptie, Decryptie en Signaalanalyse

Onderzoek naar de opslag van historische verkeersgegevens van telecommunicatieaanbieders

KPMG Informatie Risk Management
Amstelveen, November 2004
Dit rapport heeft 80 pagina's
RP/AS/ag
R.2004.TA.58.new.doc

© 2004 KPMG EDP Auditors N.V., lid van KPMG International, een Zwitserse coöperatie.
Alle rechten voorbehouden.

Inhoudsopgave

Summary (samenvatting)

Introduction

Law enforcement authorities need to use traffic data representing the usage of services of internet and telecommunication providers for law enforcement purposes. A decision should be made on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of investigation, detection and prosecution of crime and criminal offences including terrorism.

A draft framework has been developed and presented during the Justice & Internal Affairs Council held in April 2004. Dutch law enforcement authorities should determine the way in which they intend to design and implement the storage of traffic data and the data inquiry process. For this purpose, two options have been defined. Option 1 deals with telecommunication and internet providers being responsible for storage and inquiry. Option 2 reflects the situation in which storage and inquiry are arranged by the government. An example of such implementation is the Dutch Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT, hereinafter referred to as the government agency) acting as information broker in the Netherlands.

Objective

The Dutch Ministry of Justice initiated this study aimed at gaining insight into the advantages and disadvantages associated with the two options. This insight concerned the aspects related to the costs of storage and inquiry of traffic data and the impact of increasing the volume of the traffic, the security, and law and legislation. This study was mainly based on the report of Stratix Consulting Group B.V. (hereinafter referred to as Stratix-report) in June 2003. The study assumes two data retention periods, i.e. 12 months and 24 months.

Costs

To estimate the costs related to the both options 1 and 2, a distinction is made between the initial investment and the annual operational costs. These costs were estimated for the five telecommunication and internet services as described in the Stratix-report. The estimations relate to the storage and the inquiry of traffic data.

For option 1, the representative samples are one fixed network provider with approximately 70% market share, one mobile communication provider with approximately 30%-40% market share, one provider of internet services including electronic mail with approximately 10% market share and one internet café[1] with approximately 1% market share.

[1] Internet cafés are not considered to be a provider according to the Telecommunication Law. They were included in this study for the sake of completeness.

In table I, the costs are shown for the two retention periods, and a traffic volume of 100% (based on Stratix-report), an increase of 25% for the telecommunication services and an increase of 100% for the internet services.

Option 1, costs for one provider	**Market share**	**Retention period 12 months (in €)**			**Retention period 24 months (in €)**		
		Traffic 100%	**Traffic 125%**	**Traffic 200%**	**Traffic 100%**	**Traffic 125%**	**Traffic 200%**
Initial investment:							
- Fixed network	70%	18,144	19,794		28,824	31,024	
- Mobile	30-40%	23,324	25,524		31,024	48,618	
- Internet access	10%	1.5-2 M		2.2-3 M	2.2-3 M		3-4 M
- E-mail	10%	25,524		48,618	48,618		97,236
- Internet café	1%	2,730		2,730	2,730		2,730
Annual operational costs:							
- Fixed network	70%	40,000	40,000		40,000	40,000	
- Mobile	30-40%	80,000	80,000		80,000	80,000	
- Internet access	10%	20,000		20,000	20,000		20,000
- E-mail	10%	20,000		20,000	20,000		20,000
- Internet café	1%	8,000		8,000	8,000		8,000

Table I. Estimated costs of option 1 for one provider with the market share mentioned, for the two retention periods and three different traffic volumes (100% is the volume mentioned in the Stratix-report).

With regard to the costs of the initial investments, there is a direct relation between the amount of traffic data and the necessary storage capacity. New legislation may require storing more traffic data, resulting in the need for a larger storage facility for which additional costs need to be made. As the providers are adequately equipped, they are capable of storing the traffic data for a longer period than necessary for their daily business operations with limited costs. The amount of traffic data has been estimated during this study. It was noted that one deals with high-volume data storage in the event of internet access. Therefore, an advanced storage capacity is necessary which is more complex than a regular solution for data retention.

The annual operational costs of the telecommunication services are mainly related to personnel costs required for the inquiry of traffic data. For these costs estimations, the annual salary of civilian personnel is used who are employed by the Dutch government for high-level administrative job. The number of employees is determined by the quality aspects negotiated between the law enforcement authorities and the providers with regard to the inquiry process, i.e. the response time in relation to the number of inquiries. In this study, estimations and assumptions are used since there is currently no formal agreement between those two parties. The remaining part of the operational costs is related to maintaining the storage facility. As the providers run massive operations, they are able to operate the storage capacities with limited costs.

In option 2, the providers transfer the traffic data to the government agency. This organization will store the data and make it accessible for inquiry.

Option 2, storage and inquiry managed by government	**Retention period 12 months (in €)**			**Retention period 24 months (in €)**		
	Traffic 100%	**Traffic 125%**	**Traffic 200%**	**Traffic 100%**	**Traffic 125%**	**Traffic 200%**
Initial investment:						
- Fixed network	286,893	300,340		305,560	333,023	
- Mobile	93,085	98,387		154,347	182,374	
- Internet access	7 M		10 M	10 M		17 M
- E-mail	260,000		520,000	520,000		1 M
- Internet café	49,354		93,085	93,085		154,347
Annual operational costs:						
- Fixed network	422,000	422,000		472,000	489,000	
- Mobile	167,000	167,000		317,000	367,000	
- Internet access	1 M		1.5 M	1.5 M		2.2 M
- E-mail	100,000		150,000	150,000		220,000
- Internet cafe	50,000		167,000	100,000		317,000

Table II. Estimated costs of option 2, in which the process is managed by the government (the 100% traffic volume deals with the information in the Stratix-report).

The investment costs of the option 2 are influenced by three major aspects. The first aspect concerns the costs associated with the development of applications by the government agency to respond to the information requests. These costs are included in the investment for the fixed network service, assuming that these applications will be capable of delivering every type of traffic data. The second aspect deals with components for the infrastructure required to collect, transfer and store the data. The third aspect relates to the required storage capacity as the total traffic data per telecommunication service is stored by the government agency. If the amount of traffic increases, e.g., by 25% for telecommunication via fixed or mobile network, and by 100% for internet, the investment costs for storing the traffic data is virtually linear with the amount of stored data. Therefore, a 25% or 100% increase in traffic results in a 25% or 100% increase in the third aspect of the investments.

In addition to other aspects, one factor has a major impact on the operational costs of option 2. It concerns the annual fee currently paid by the Dutch government to the Dutch telecommunication providers for delivering the data. This amount is calculated once for the fixed network services as it also covers delivering the data for the other types of the telecommunication and internet services.

The costs of handling the inquiries are, in fact, relatively independent of the amount of stored data. The number of inquiries is the result of the activities of law enforcement authorities, and their volume is determined by the actual threat level and the number and complexity of their investigations.

Security aspects

As the traffic data contains privacy-related personal details, the Dutch law regarding their protection (i.e. WBP) applies. This law requires three security aspects to be taken into consideration when dealing with those details: confidentiality, integrity and continuity. The WBP defines four 'risk classes' indicating the level of the required security measures. For this study, the highest risk class was applied.

For option 1, attention was also paid to the security article of the Telecommunication Law and to the informal agreements made between the government and the providers with respect to security when tapping the communication. During a tap operation, both user data and traffic data are known to the investigator. The informal security agreements cover the quality aspects defined by the WBP and pay adequate attention to other important aspects including audits and costs. Therefore, they can also be applied as a model for securing the traffic data.

For option 2, sessions were organized in which the government agency participated. It became clear that this agency has followed and currently implements the government security regulations, and also put emphasis on other aspects including audits and costs. In addition, there is an on-going effort to comply with the highest security regulation intended for securing special information within the government. A considerable number of the corresponding measures are currently implemented. As these security measures exceed the WBP, it can be said that the security aspects defined by this law are met by the government agency.

Law & legislation

Currently, the providers store user data into the black boxes. The providers remain the owners of the data stored therein, while the government executes the inquiries on the content of the black boxes. This situation is in compliance with the current law and legislation.

This study deals with extending the process of collecting user data and making traffic data accessible to the inquiry process. This will result in a substantial increase of the volume of stored data. The question arises whether this combined data should stay on the premises of the providers under their ownership, or should be handed over to the government. Moving the ownership from the providers to the government implies usage of the data for other purposes than for which it was collected by the providers. This requires the adaptation of the law allowing the government to use this data to persecute criminal activities.

Future steps

It is necessary to nominate a project group for the realization of the selected option. This group needs to identify a sponsor and initiate activities including the following two important actions. The first one concerns defining the information needs of the law enforcement authorities which is the starting point for designing the required storage and inquiry facility. The second action is related to performing an impact analysis.

It should be aimed at providing detailed information regarding the impact on the processes and the infrastructure in use by the telecommunication providers and the government agency.

Moreover, a choice should be made about the ownership of the data. If it is decided to let the data be owned by the government, an adaptation of the law is required.

Remarks

For the inquiry process, one may decide to implement an automated process or to handle the inquiries manually. In the event of an automated process, an initial investment is required to design and implement an application. Within the limits of the capacity of the application, the number of inquiries will not result in additional variable costs. On the other hand, if a manual process is selected, the investment costs are relatively low, but the government has to pay for each transaction. In option 1, the providers will charge for each inquiry, while in option 2 the appropriate number of employees must be hired. The variable costs of the manual process depend upon the volume of the inquiries and the price per inquiry.

It should be noted that the current technological developments make it possible to store and inquiry massive amounts of data easier than in the past. The storage technology improves continuously and provides the possibilities to access high-volume data faster in comparison with the facilities currently in use. In addition, there are technological concepts launched on the market using more sophisticated compression techniques. Using them, it is possible to save approximately 70% on the storage capacity.

Should you have any further questions, please do not hesitate to contact us.

Yours sincerely,

Prof. dr. ir. R. Paans RE

1 Inleiding

1.1 Achtergrond

De Europese Raad heeft in haar verklaring van 25 maart 2004, aangaande de bestrijding van terrorisme, de opdracht gegeven voorstellen te bestuderen voor het opstellen van voorschriften voor het bewaren van de historische verkeersgegevens[2] van de telecommunicatieaanbieders. Deze voorschriften dienen voor 1 juni 2005 ten behoeve van de besluitvorming te worden voorgelegd aan de Europese Raad. Tijdens de JBZ Raad van 28 en 29 april 2004 hebben het Verenigd Koninkrijk, Frankrijk, Ierland en Zweden een ontwerp kaderbesluit gepresenteerd. Dit ontwerp zal nader worden uitgewerkt tot het gevraagde voorstel waarop besluitvorming kan plaatsvinden. Dit houdt in dat op korte termijn uitsluitsel dient te worden gegeven omtrent de wijze waarop de opsporings-, Inlichtingen- en Veiligheidsdiensten (hierna: behoeftestellers) in Nederland het bewaren van verkeersgegevens vorm willen geven. Daarbij is het van belang de haalbaarheid van de verschillende concepten alsmede de hiermee gepaard gaande kosten te onderkennen.

De onderzoeken van de behoeftestellers vinden plaats binnen de wettelijke kaders van het Wetboek van Strafvordering en de Wet op de Inlichtingen- en Veiligheidsdiensten. De vereiste medewerking van de telecommunicatiebedrijven is nader uitgewerkt in de Telecommunicatiewet. Welke gegevens mogen worden gevorderd door de behoeftestellers bij de telecommunicatieaanbieders is aangegeven in de besluiten[3] Vorderen Verkeersgegevens. Belangrijk daarbij is welke kosten met het bewaren en het bevragen van de historische verkeersgegevens zijn gemoeid. Het ontwerp Kaderbesluit gaat uit van een minimale bewaartermijn van 12 maanden en een maximale bewaartermijn van 36 maanden. Het Nederlandse standpunt tendeert naar een bewaartermijn van 12 maanden.

1.2 Opdrachtomschrijving

Voor de opslag en de bevraging van de historische verkeersgegevens dienen zich 2 opties aan. De eerste optie (optie 1) reflecteert de situatie waarbij de telecommunicatieaanbieders de opslag en de bevraging van de historische verkeersgegevens volledig voor hun rekening nemen. De tweede optie (optie 2) geeft de situatie weer waarbij de overheid volledig zorgdraagt voor het opslaan en het bevragen van de historische verkeersgegevens.

[2] Onder verkeersgegevens wordt verstaan de gegevens over de gebruiker en over het telecommunicatieverkeer met betrekking tot deze gebruiker. Dit begrip is ruimer dan het begrip zoals dat in het verband met de Telecommunicatiewet wordt gehanteerd, aangezien het (onder meer) mede de zogenaamde gebruikersgegevens omvat. Dat zijn de gegevens betreffende de naam, adres, woonplaats, nummer en soort dienst.
[3] Aan de Inlichtingen- en Veiligheidsdiensten kant onder WIV dat ten tijde van dit onderzoek nog niet in werking was getreden; onder strafvordering valt het besluit dat per 1 september 2004 van kracht is geworden.

Bij beide opties dient rekening te worden gehouden met een aantal aspecten, te weten de investerings- en de beheerkosten, en de wijze van beveiliging, zowel bij de opslag als bij de bevraging van de verkeersgegevens. Bij optie 2 kan worden gedacht aan de opzet van een systeem van gedecentraliseerde databases. Deze kunnen worden bevraagd door een centraal zoeksysteem dat door de overheid wordt beheerd. Aangezien dit idee vergelijkbaar is met het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)-concept, is CIOT (hierna: overheidsinstantie) gedurende dit onderzoek als voorbeeld gehanteerd.

De directeur Opsporingsbeleid van het Ministerie van Justitie was als voorzitter van de interdepartementale Beleidsgroep voor Interceptie, Decryptie en Signaalanalyse, daarom voornemens een onderzoek uit te laten voeren naar de consequenties van het bewaren en bevraagbaar doen zijn van de historische verkeersgegevens door optie 1 respectievelijk optie 2. KPMG Information Risk Management (hierna: KPMG) was door het bureau Platform Interceptie, Decryptie en Signaalanalyse (PIDS) gevraagd dit onderzoek uit te voeren. Kosten en investeringen ten behoeve van de aanlevering van gegevens aan de aanbiederkant zijn niet onderzocht.

1.3 Opdrachtdoelstelling

Doel van deze opdracht was een beter inzicht te verkrijgen in de voor- en nadelen van het bewaren en het bevragen van de verkeersgegevens door de telecommunicatieaanbieders, oftewel optie 1, respectievelijk door de overheid, namelijk optie 2. Dit inzicht moest tot stand komen na bestudering van de investerings- en beheerkosten en de benodigde beveiligingsmaatregelen. De opdracht diende te worden uitgevoerd uitgaande van een bewaartermijn van 12 maanden en uitgaande van een bewaartermijn van 24 maanden. Daarbij waren de onderstaande vragen van belang:

- Wat zijn de geraamde kosten van beide opties?
- Wat zijn de beveiligingsaspecten voor beide opties?
- Volstaat de huidige wet- en regelgeving om het bewaren van verkeersgegevens door de overheid te laten uitvoeren?
- Wat zijn de consequenties voor het bewaren en bevraagbaar maken van verkeersgegevens indien het telecommunicatieverkeer met 25% en het internetverkeer met 100% (verdubbeling) toeneemt?
- Wat zijn de organisatorische consequenties voor de aanbieders en voor de overheid?
- Hoe zien de vervolgstappen eruit voor de realisatie van de 2 onderzochte opties?

De opdracht resulteerde in een rapport van bevindingen omtrent de consequenties voor de aanbieders en voor de overheid bij een opslag en bevraagbaar doen zijn van de historische verkeersgegevens bij telecommunicatie.

Het rapport bevat tevens een plan van aanpak voor de realisatie van de 2 onderzochte opties. Het onderzoek is voornamelijk gebaseerd op het Stratix-rapport en is los van de telecommunicatieaanbieders uitgevoerd. Waar nodig zijn aannames gemaakt en gedocumenteerd.

1.4 Aanpak

Voor de uitvoering van deze opdracht is een aanpak bestaande uit 8 fasen gehanteerd, die hieronder nader worden beschreven. Het onderzoek is in de periode juni 2004 tot en met oktober 2004 uitgevoerd.

Fase 1: Kick-off & initiatie

In deze fase is een bijeenkomst georganiseerd waarin KPMG de onderzoekaanpak nader toelichtte, werkafspraken maakte en de beschikbare documentatie in ontvangst nam. Tijdens deze kick-offsessie werd aangegeven dat het bureau PIDS de onderzoekvraagstelling coördineerde. Dit bureau werd derhalve gedurende het onderzoek frequent door KPMG gecontacteerd teneinde de verwachtingen adequaat te managen. Tevens werd overeenstemming bereikt over de zogeheten 'begeleidingsgroep'. Deze groep werd op de hoogte gehouden van de voortgang van de opdracht. Met hen werd tevens de opgeleverde deliverables besproken, waarvoor 5 sessies gedurende de onderzoekperiode werden georganiseerd. De begeleidingsgroep bestond uit de vertegenwoordigers van het Ministerie van Economische Zaken, Ministerie van Binnenlandse Zaken & Koninkrijksrelaties, Ministerie van Justitie, Openbaar Ministerie en Politie.

In overleg met de opdrachtgever werden daarnaast de contactpersonen en de geïnterviewde personen aan de kant van het ministerie bepaald.

Fase 2: Geraamde kosten

Voor de berekening van de geraamde kosten van optie 1 en optie 2 is de door KPMG ontwikkelde ICT-investeringsanalyse toegepast. Met behulp van deze methode werden de ICT-kostencomponenten in kaart gebracht, waarin wordt geïnvesteerd ter ondersteuning van het bewaren en het bevragen van de historische verkeersgegevens door de overheid en door de telecommunicatieaanbieders.

Onderscheid is gemaakt tussen 2 soorten kosten, te weten: incidentele kosten en doorlopende kosten. Het eerstgenoemde heeft betrekking op de vaste kosten die éénmalig en direct worden gemaakt waaraan hierna als investeringskosten wordt gerefereerd. Deze kosten omvatten de componenten geassocieerd met de aanschaf van softwarelicenties (hierna: softwarelicenties), uitbreiding of vernieuwing van de hardware (hierna: hardware), wijziging van de bestaande applicaties (hierna: wijziging applicaties), ontwikkeling van nieuwe applicaties (hierna: nieuwe applicaties), upgrades, aankoop van back-upmedia (hierna: back-upmedia), uitwijk ten behoeve van calamiteiten (hierna: uitwijk) en installatie van de aanpassingen in de operationele omgeving (hierna: installatie). Hierin is niet meegenomen de vervanging na het verlopen van de technische en/of economische levensduur van de componenten.

De doorlopende kosten betreffen de variabele kosten die een terugkerend karakter bezitten. Deze worden hierna aangeduid als exploitatie- en beheerkosten, en bevatten de componenten betreffende eigen personeel (hierna: personeel) of inhuur van externen ten behoeve van het technisch onderhoud en dagelijkse operatie, huisvesting en huur van de datacommunicatielijnen (hierna: huurlijnen).

Fase 3: Beveiligingsaspecten

Aangezien de historische verkeersgegevens onder meer persoongegevens[4] betreffen, dienen deze conform de Wet Bescherming Persoongegevens (WBP) te worden beveiligd. In het kader van deze wet kent de beveiliging van persoongegevens drietal kwaliteitsaspecten, te weten: exclusiviteit, integriteit en continuïteit. Voor een adequaat beveiligingsniveau is het essentieel de risicoklasse (risicoklasse 0 t/m risicoklasse 3) van persoonsgegevens te bepalen. Afgesproken was in samenspraak met de begeleidingsgroep vast te stellen welke risicoklasse op de historische verkeersgegevens van toepassing is. Deze keuze is doorslaggevend voor het definiëren van de maatregelen om de beveiliging van die gegevens te waarborgen waarbij tevens het artikel 13.5 van de Telecommunicatiewet alsmede de bijbehorende AMVB in acht wordt genomen. Er is gesproken over de processen (aanlevering, opslag en bevraging) waarin de verkeersgegevens worden verwerkt. Hierbij werd rekening gehouden met optie 1 en optie 2. De aard van de verkeersgegevens alsmede het doel waarvoor deze worden gebruikt, zijn vervolgens besproken. Hierna kwamen de beveiligingsissues voor optie 1 en voor optie 2 aan de orde.

Fase 4: Organisatievorm optie 2

Op verzoek van de opdrachtgever zijn 3 scenario's gepresenteerd als mogelijke organisatievormen voor optie 2, te weten: centrale opslag en bevraging binnen hetzelfde domein, gescheiden opslag en bevraging binnen hetzelfde domein en gescheiden opslag en bevraging binnen verschillende domeinen.

Fase 5: Wet- en regelgeving

In deze fase is onder andere aandacht besteed aan de specifieke aspecten van de privacyrichtlijn. Tevens is rekening gehouden met het opvragen van informatie tussen lidstaten onderling (artikel 5 van het ontwerp kaderbesluit). De discussie ging in op de geformuleerde vraag of er wettelijke belemmeringen zijn om historische verkeersgegevens zoals deze dienen te worden bewaard door de telecommunicatieaanbieders, te laten bewaren door/bij de overheid in plaats van door/bij de aanbieder zelf.

[4] Persoongegeven is in het kader van WBP gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Fase 6: Consequenties toename telecommunicatieverkeer met 25% en internetverkeer met 100%

Deze fase richtte zich op een mogelijke toename van 25% in het telecommunicatieverkeer en toename van 100% in het internetverkeer. Rekeninghoudend hiermee is eerst de organisatorische impact van de hierboven genoemde toename op de telecommunicatieaanbieders en op de overheid inzichtelijk gemaakt. Na deze analyse werd gekeken wat de technische consequenties waren om aan de geschatte toename te voldoen. Hierbij werd in het bijzonder de nadruk gelegd op de infrastructurele aspecten.

Fase 7: Vervolgstappen

De focus van deze fase was een beschrijving van de te nemen vervolgstappen teneinde de onderzochte opties te realiseren. De te volgen organisatorische en technische stappen werden aangegeven tezamen met de daarbijbehorende prioriteiten, tussenstappen, communicatiekanalen met de belanghebbenden, benodigde mensen en middelen, planning en deliverables. Waar nodig en gewenst zijn pragmatische adviezen aangereikt.

Fase 8: Afstemming & afronding

In deze fase werden de gedurende het onderzoek opgeleverde tussenrapportages samengevoegd en het conceptrapport opgesteld om met de opdrachtgever af te stemmen. De samenvatting van het eindrapport is in het Engels opgesteld.

1.5 Indeling rapport

Dit rapport is als volgt ingedeeld. Hoofdstuk 2 geeft een overzicht van de voor dit onderzoek geldende uitgangspunten en aannames. De met optie 1 en optie 2 gepaard gaande kosten zijn in Hoofdstuk 3 geschat en onderbouwd. De gevolgen van de toename van het telecommunicatieverkeer zijn eveneens daarin gepresenteerd. Hoofdstuk 4 beschrijft de beveiligingsaspecten betreffende deze 2 opties. Hoofdstuk 5 analyseert of de huidige wet- en regelgeving het bewaren van de historische verkeersgegevens door de overheid toelaat. De vervolgstappen voor de realisatie van optie 1 alsmede optie 2 zijn in hoofdstuk 6 uitgewerkt. Hoofdstuk 7 geeft een beknopte reflectie van de huidige technologische ontwikkelingen op de markt tezamen met een raming van de bijbehorende kosten waar mogelijk.

Bij dit rapport zijn 2 bijlagen gevoegd. Bijlage A geeft een overzicht van de bestudeerde documentatie en van de geïnterviewden. In Bijlage B is een opsomming van de in dit rapport gebruikte afkortingen gepresenteerd.

2 Onderzoeksuitgangspunten en -aannames

In deze paragraaf worden de in het kader van dit onderzoek gehanteerde uitgangspunten en gemaakte aannames beschreven.

2.1 Uitgangspunten

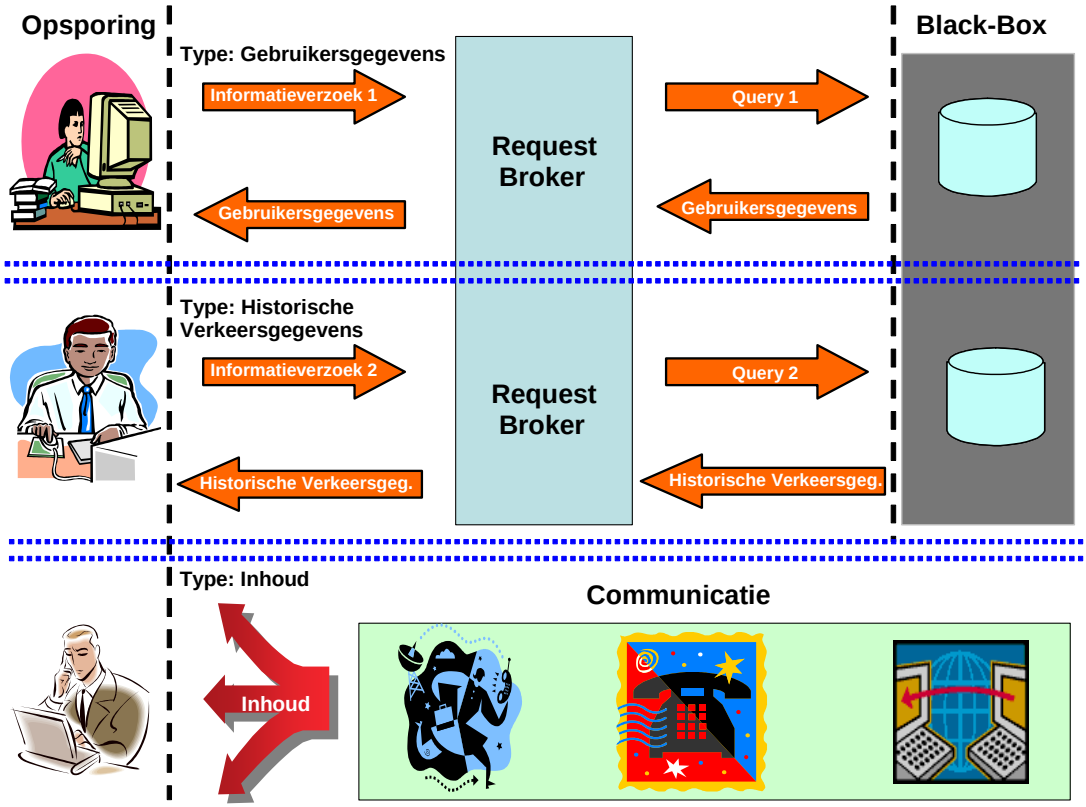
Het in juni 2003 uitgebrachte Stratix-rapport is bij het onderzoek als uitgangspunt gehanteerd. Daarin zijn de uitkomsten opgenomen van het onderzoek naar de beschikbaarheid van de verkeersgegevens bij de telecommunicatieaanbieders (hierna: Stratix-onderzoek) dat op 26 maart 2002 was gestart. De onderstaande diensten zijn daarbij onderzocht:

- vaste telefonie;
- mobiele telefonie;
- internettoegang;
- e-mail;
- toegang tot internet via internetcafés.

In dit kader wordt onderscheid gemaakt tussen 3 type gegevens, te weten:

- Gebruikersgegevens. Hiermee worden de gegevens bedoeld zoals naam, adres, woonplaats, nummer en geabonneerde dienst.
- In het Stratix-rapport wordt onder historische verkeersgegevens verstaan gegevens aangaande het gebruik van netwerken en diensten in het verleden. In het ontwerp ‘Besluit vorderen gegevens telecommunicatie’ wordt de term verkeersgegevens anders gepositioneerd. Deze wordt omschreven als gegevens over de gebruiker plus het telecommunicatieverkeer aangaande deze gebruiker; dit is dus de combinatie van gebruikersgegevens en verkeersgegevens. In dit onderzoek wordt verder de definitie van het Stratix-rapport gehanteerd.
- Inhoud van de communicatie waarbij er sprake is van het afluisteren van de communicatie. Deze type gegevens valt buiten de scope van het huidige onderzoek.

Deze 3 type gegevens zijn in figuur 1 schematisch weergegeven.



Figuur 1. Verschillende typen gegevens. Dit onderzoek richt zich op de historische verkeersgegevens.

In het Stratix-rapport is tevens aangegeven dat de geschatte gegevensvolumes uitgaan van een bewaartermijn van 12 maanden. Conform de onderzoeksvraagstelling is dit onderzoek uitgevoerd uitgaande van zowel een bewaartermijn van 12 maanden als 24 maanden voor het opslaan en het bevragen van de historische verkeersgegevens.

Het Stratix-rapport beschrijft dat de telefonieaanbieders doorgaans ervaring hebben met het meewerken aan de door de behoeftestellers ingediende verzoeken en vorderingen. Deze vragen zijn divers van aard en variëren van het opzoeken van gegevens op basis van identiteit (bijvoorbeeld een telefoonnummer) en datum/tijd tot complexe analyses. In tegenstelling tot de telefonieaanbieders blijken de Internet Service Provders (ISPs) volgens het Stratix-rapport in zeer beperkte mate verzoeken en vorderingen te ontvangen van de behoeftestellers. Verwacht wordt dat het aantal vragen zal toenemen. De telefonieaanbieders hebben het proces ten behoeve van de informatieverstrekking, mede door de frequente verzoeken en vorderingen, beter ingericht dan ISPs. Het Stratix-rapport geeft tevens aan dat de telefonieaanbieders zich meer bewust zijn van de regels.

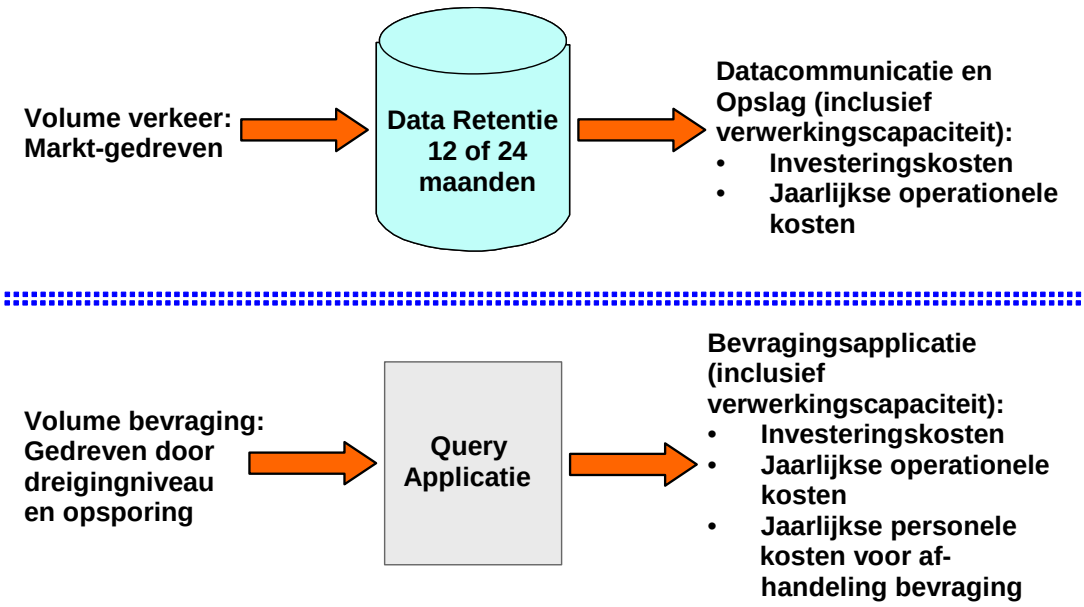
2.2 Aannames

Aangenomen is dat de telecommunicatieaanbieders de benodigde uitbreidingen ten gevolge van het ontwerp 'Besluit vorderen gegevens telecommunicatie' niet combineren met andere noodzakelijke veranderingen, en geen gebruikmaken van de schaalvoordelen die kunnen ontstaan indien de aanbieders gezamenlijk een oplossing realiseren teneinde te voldoen aan deze wettelijke verplichting. Tevens is verondersteld dat uitsluitend het internetverkeer een explosieve groei zal realiseren. Het verkeersvolume aangaande andere telecommunicatiediensten blijft relatief stabiel.

De snelheid (responsetijd) waarmee de telecommunicatieaanbieders de verkeersgegevens dienen te leveren is nog niet concreet uitgedrukt in termen van minuten, uren of dagen. Onder meer artikel 3 van Algemene Inrichtingseisen van de 'Regeling aftappen openbare telecommunicatienetwerken en -diensten' beschrijft dat de aanbieder van een openbaar telefoonnetwerk, onderscheidenlijk een vaste openbare telefoondienst, zijn netwerk, onderscheidenlijk zijn dienst, zodanig inricht dat iedere bijzondere last '*onverwijld'* kan worden uitgevoerd. Deze term wordt doorgaans geïnterpreteerd als 'zo spoedig mogelijk' hetgeen concreet inhoudt dat de aanbieder de benodigde activiteiten initieert zodra een informatieverzoek binnenkomt. Vorderingen dienen tenminste één van de gegevens te bevatten die zijn genoemd in de Algemene Inrichtingseisen van de 'Regeling aftappen openbare telecommunicatienetwerken en -diensten'. De responsetijd en werklast hebben een grote invloed op de geraamde kosten van optie 1 en optie 2, hetgeen voor de toekomstige situatie nog niet is geconcretiseerd.

Thans wordt op de bij de telecommunicatieaanbieders binnenkomende informatieverzoeken binnen maximaal 5 werkdagen gereageerd. Gedurende het onderzoek bleek dat er geen volledig beeld bestond van het exacte aantal informatieverzoeken. Dit aantal was slechts bekend voor 2 grote en voor 3 kleine korpsen. Aangenomen is dat circa 600 verzoeken per maand door een vaste telefonieaanbieder en ongeveer 1.400 verzoeken per maand door een mobiele aanbieder worden afgehandeld. Hierbij is rekening gehouden met de groei van de mobiele telefonie. Tevens is verondersteld dat circa 10 verzoeken per maand bij een aanbieder binnenkomen aangaande de internetgerelateerde diensten. Het hierboven genoemde aantal informatieverzoeken is op basis van een steekproef vastgesteld.

De opslag en de bevraging worden als 2 separate dimensies beschouwd. De toename van het verkeersvolume is marktgedreven en heeft direct invloed op de opslagcapaciteit. Dit houdt concreet in dat de verkeerstoename additionele opslagruimte vergt. In feite is deze stijging onafhankelijk van de bevragingsfrequentie. Deze wordt gedreven door het dreigingsniveau en door de behoeftestellers. Dit wil zeggen dat de toename van het verkeersvolume niet direct zal resulteren in de stijging van het aantal bevragingen. De toename van deze frequentie kan wel leiden tot additionele behoefte aan menskracht. Deze 2 dimensies zijn in figuur 2 schematisch weergegeven.



Figuur 2. Opslag en bevraging als 2 aparte onafhankelijke dimensies voor het bepalen van de kosten.

3 Geraamde kosten

De geraamde kosten van optie 1 en optie 2 zijn hieronder separaat uitgelegd, waarbij de uitgangspunten aangaande de bewaartermijnen in acht zijn genomen. Een totaal overzicht van deze geschatte kosten is eveneens gepresenteerd. Kosten geassocieerd met een component zijn als 'nihil' aangegeven indien deze marginale financiële impact hebben, geen gegevens daarover zijn opgenomen in het Stratix-rapport, aannames daaromtrent zijn gemaakt of zijn reeds meegerekend. Deze indicatie is in dat geval nader beargumenteerd. De met nihil aangeduide kosten zijn in de ramingcalculatie van opties 1 en 2 als '0' meegerekend. Een apart te berekenen kostencomponent is als subonderdeel vermeld. Deze indicatie is in dat geval tevens beargumenteerd. Opgemerkt wordt dat de aangegeven prijzen exclusief BTW zijn.

In dit hoofdstuk worden de organisatorische en technische consequenties voor het bewaren en bevraagbaar maken van de verkeersgegevens eveneens beschreven in geval het telecommunicatieverkeer toeneemt. De bijbehorende kosten zijn eveneens geschat en beschreven.

3.1 Scope

Bij de berekening van de geraamde kosten van optie 1 en optie 2 is geen rekening gehouden met de kosten (zoals IT en personeelgerelateerde kosten) die gaan gepaard met het opstellen en het indienen van de informatieverzoeken door de behoeftestellers. Berekeningen van de geraamde kosten van de beide opties betreffen de daadwerkelijke opslag en bevraging van de historische verkeersgegevens teneinde te voldoen aan de door de behoeftestellers ingediende informatieverzoeken. Tevens maakten de afschrijvingsmethoden geen deel uit van de bij deze fase behorende activiteiten, en zijn derhalve niet onderzocht. De administratieve kosten die in het kader van de Telecommunicatiewet door de aanbieders en door de ISPs worden gemaakt, vallen buiten de scope van deze fase.

Het Stratix-rapport concludeert dat de aanbieders van de telecommunicatiediensten een groot deel van de informatie kunnen leveren waaraan de behoeftestellers behoefte hebben. Additionele gegevensregistratie is nodig om hen volledig te voorzien in hun informatiebehoefte hetgeen de toename van de gegevensopslag tot gevolg heeft. Hiermee is geen rekening gehouden bij de berekening van de geraamde kosten bij opties 1 en 2. De argumentatie hiervoor heeft een duaal karakter. Enerzijds is de omvang van de additionele gegevensregistratie niet onderzocht. Anderzijds is er geen harde zekerheid omtrent de beschikbaarheid en betrouwbaarheid van de verkeersgegevens. Veel ISPs maken geen back-ups van de gelogde gegevens, en accepteren voor hun eigen bedrijfsvoering dat de logs soms verloren gaan.

3.2 Optie 1: opslag en bevraging bij de provider

Per telecommunicatiedienst is de totstandkoming van de geraamde investerings- en exploitatie- en beheerkosten voor deze optie in de volgende secties uiteengezet. Waar mogelijk zijn deze kostenschattingen tevens per bewaartermijn gecalculeerd en toegelicht. Kostencomponenten zijn voor de bewaartermijn van 12 maanden beschreven. Voor de bewaartermijn van 24 maanden zijn met name de relevante componenten uitgelegd.

3.2.1 Vaste telefonie

In het kader van het Stratix-onderzoek is één aanbieder van de vaste telefonie geïnterviewd.

3.2.1.1 Uitgaande gesprekken

De aanbieder van de vaste telefonie met 70%[5] (onder meer lokaal en nationaal) marktaandeel bewaart de verkeersgegevens over de uitgaande en beantwoorde gesprekken inclusief gratis gesprekken (0800) en gesprekken die via andere operators lopen (Carrier Select en Carrier Pre-Select) voor 5 maanden. Per dag worden naar verwachting 35 miljoen records gegenereerd, waarvan 110 bytes per record worden vastgelegd. Dit resulteert in de dagelijkse registratie van circa 4 gigabyte (GB) verkeersgegevens (35 miljoen x 110 bytes). Deze aanbieder slaat momenteel standaard 0,6 terabyte (TB) op en heeft voor deze 5 maanden (5 maanden x 30 dagen X 4GB per dag) opslagruimte nodig.

De uitbreiding naar de bewaartermijn van 12 maanden houdt in dat de verkeersgegevens 7 maanden langer dienen te worden bewaard door de aanbieder. Voor deze extra bewaartermijn is circa 0,9TB (7 maanden x 30 dagen x 4GB per dag) opslagcapaciteit noodzakelijk.

Ten behoeve van de bewaartermijn van 24 maanden is ongeveer 2,3TB opslagruimte (12 maanden + 7 maanden x 30 dagen x 4GB per dag) nodig om de uitgaande en beantwoorde gesprekken inclusief gratis gesprekken (0800) en gesprekken die via andere operators lopen (Carrier Select en Carrier Pre-Select) op te slaan.

3.2.1.2 Binnenkomende gesprekken

Binnenkomende gesprekken vanuit andere netwerken worden door de aanbieder van de vaste telefonie met 70% marktaandeel in andere centrales geregistreerd dan de centrales waarin de uitgaande gesprekken worden vastgelegd. In het Stratix-rapport is geen indicatie gegeven van het verkeersvolume en de bewaartermijn betreffende de binnenkomende gesprekken. Uitgaande van het hierboven genoemde marktaandeel heeft de gehele markt 50 miljoen (35 miljoen / 70% marktaandeel) uitgaande gesprekken. Dit houdt concreet in dat per dag naar verwachting 15 miljoen (50 miljoen - 35 miljoen) records bij de andere aanbieders worden gegenereerd.

[5] Bron: persberichten, KPN sluit succesvol kwartaal af met een winst na belastingen van EUR 375 miljoen, Den Haag, 10-05-2004.

Van deze gesprekken komen 10,5 miljoen (15 miljoen x 70% marktaandeel) binnen bij de vaste telefonieaanbieder. Dit leidt tot de dagelijkse registratie van circa 1,2GB (10,5 miljoen x 110 bytes) verkeersgegevens. Aangenomen is dat de vaste telefonieaanbieder ten behoeve van de binnenkomende gesprekken een standaard opslagtermijn van 5 maanden hanteert.

De uitbreiding naar de bewaartermijn van 12 maanden betekent dat de verkeersgegevens 7 maanden langer dienen te worden bewaard. Voor deze additionele bewaartermijn is ongeveer 0,3TB (7 maanden x 30 dagen x 1,2GB per dag) opslagruimte nodig.

Voor de bewaartermijn van 24 maanden is circa 0,7TB (12 maanden + 7 maanden x 30 dagen x 1,2GB per dag) opslagcapaciteit noodzakelijk om de binnenkomende gesprekken op te slaan.

Hierbij zijn de binnenkomende gesprekken van mobiel naar vast niet meegenomen.

3.2.1.3 Call attempts

De in het Stratix-onderzoekgenoemde aanbieder van de vaste telefonie registreert de 'Call Attempts' geheel niet. Een registratieplicht voor deze onbeantwoorde oproepen zal niet alleen gevolgen hebben voor de wijze waarop de verkeersgegevens worden opgeslagen, maar ook voor de onderliggende telecommunicatie-infrastructuur (zoals aanpassingen in de bestaande applicaties en centrales). Aangezien de harde cijfers omtrent het volume van de onbeantwoorde oproepen ontbreken en geen inzicht bestaat in de structuur en complexiteit van de infrastructuur, hebben de financiële consequenties voor de beschikbaarstelling van die verkeersgegevens geen onderdeel uitgemaakt van de berekening van de geraamde kosten.

3.2.1.4 Totale opslagcapaciteit bij de gekozen aanbieder

Voor de bewaartermijn van 12 maanden wordt de extra benodigde capaciteit voor de opslag van de uitgaande gesprekken alsmede de binnenkomende gespreken geschat op 1,2TB (0,9TB + 0,3TB). Dit betreft 7 maanden extra opslag ten opzichte van de 5 maanden die de vaste telefonieaanbieder nu hanteert.

Voor de bewaartermijn van 24 maanden is 3TB (2,3TB + 0,7TB) extra opslagruimte nodig om de gesprekken op te slaan.

3.2.1.5 Investeringskosten

Aangezien de aanbieder van de vaste telefonie met circa 7 miljoen klanten vrijwel de meeste vaste aansluitingen vertegenwoordigt, is verondersteld dat het gebruik van databases en hun upgrades ten behoeve van de opslag van de verkeersgegevens nauwelijks additionele licentiekosten tot gevolg heeft. De argumentatie voor deze aanname is dat de meeste soortgelijke grote organisaties in het algemeen grootschalig softwarelicenties inkopen en langdurige contracten afsluiten met als doel lage prijsafspraken te maken. Hierdoor kunnen extra benodigde licenties direct worden gebruikt waarvoor in feite reeds is betaald.

Grotendeels gelden dergelijke kortingsregelingen eveneens voor de hardware en de bijbehorende service. Mede door de snelle ontwikkeling van de hardwaretechnologie en de verbetering van de prijs/prestatie verhouding wordt de hardware niet vooraf ingekocht. Op het moment dat deze nodig is, wordt de bestelling bij de hardwareleverancier geplaatst. Een ruwe indicatie conform de prijsopgave van een leverancier voor een server met de opslagcapaciteit van circa 1,2TB wordt geschat op EUR 18.144. Gezien de prijsafspraken die de grote organisaties als de aanbieder van de vaste telefonie met de hardwareleveranciers maken, kunnen de kosten voor de installatie van de server als nihil worden beschouwd. Deze afspraken dekken in de meeste gevallen dergelijke kosten. De met de wijziging of nieuwe applicaties gepaard gaande kosten zijn als marginaal meegenomen aangezien de aanbieder van de vaste telefonie altijd dient te voldoen aan de Algemene Inrichtingseisen. In het Stratix-rapport zijn geen gegevens opgenomen aangaande de back-up en uitwijk. Gezien het belang van de continuïteit van de bedrijfsvoering voor de aanbieder van de vaste telefonie is aangenomen dat reeds de back-up en uitwijk zijn geregeld, waardoor additionele kosten als marginaal zijn beschouwd.

Een ruwe indicatie conform de prijsopgave van een hardwareleverancier voor een server van een bekend merk met de opslagcapaciteit van circa 3TB wordt geschat op EUR 28.824. De geraamde investeringskosten zijn in tabel 1 getoond.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	Nihil	Nihil
Hardware	EUR 18.144	EUR 28.824
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	Nihil	Nihil
Uitwijk	Nihil	Nihil
Installatie	Nihil	Nihil
Totaal:	EUR 18.144	EUR 28.824

Tabel 1. Geraamde initiële investeringskosten voor de vaste telefoniediensten van de aanbieder met 70% marktaandeel.

3.2.1.6 Exploitatie- en beheerkosten

Ten behoeve van de exploitatie- en beheerkosten voor de bewaartermijnen van 12 en 24 maanden, is ervan uitgegaan dat het beheer van het hierboven beschreven opslagsysteem onderdeel kan uitmaken van de bij de aanbieder van de vaste telefonie geïmplementeerde IT-operaties. Dit houdt concreet in dat het technische personeel van de aanbieder of de inhuur zorgdraagt voor de dagelijkse uitvoering van de daarbijbehorende werkzaamheden. Deze personeelskosten zijn een onmisbare component in de berekening van de jaarlijkse IT-kosten. Voor het opslagsysteem benodigde ruimte kan gebruik worden gemaakt van de door de aanbieder geregelde huisvesting voor haar omvangrijke IT-huishouding, waarmee in het kader van de jaarlijkse IT-kosten rekening wordt gehouden. Huurlijnen zijn al voor uiteenlopende doeleinden in gebruik die tevens ten behoeve van het opslagsysteem kunnen worden gebruikt.

De met deze lijnen gepaard gaande kosten zijn normaliter opgenomen in het jaarlijkse IT-budget. Doorgaans kan worden gesteld dat de aanbieder van de vaste telefonie in het kader van haar bedrijfsvoering reeds voor deze 4 componenten heeft betaald en nauwelijks additionele kosten hoeft te maken.

De exploitatie- en beheerkosten aangaande de bevraging beperken zich in feite tot de personeelskosten mede gezien de aangereikte argumentatie voor de resterende componenten. Uitgaande van de hierboven gemaakte aanname is er sprake van 30 (600 verzoeken / 20 dagen) binnenkomende verzoeken per dag. Verondersteld is dat 1 fte nodig is om ongeveer 30 bevragingen per dag (8 uur) te behandelen. Deze aanname is gebaseerd op de ervaringscijfers van de professionele call-centers die eveneens klanten onverwijld moeten helpen. Iedere klantenvraag wordt normaliter door een call-centeragent binnen 15 minuten behandeld of doorgestuurd voor de verdere afhandeling. Ten behoeve van het bevragingspersoneel wordt gedacht aan schaal 7 (HAVO+/VWO/MBO+ niveau voor het hoog administratief werk) met de bijbehorende integrale jaarlijkse kosten van circa EUR 40.000[6]. Hierdoor bedragen de personeelskosten EUR 40.000 per jaar. Dit bedrag is onafhankelijk van de bewaartermijn. Een overzicht van de totale exploitatie- en beheerkosten is in tabel 2 gegeven.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	Nihil	Nihil
- Bevraging	EUR 40.000	EUR 40.000
Inhuur	Nihil	Nihil
Huisvesting	Nihil	Nihil
Huurlijnen	Nihil	Nihil
Totaal:	EUR 40.000	EUR 40.000

Tabel 2. Geraamde jaarlijkse exploitatie- en beheerkosten voor de vaste telefoniediensten van de aanbieder met 70% marktaandeel.

3.2.2 Mobiele telefonie

In het kader van het Stratix-onderzoek zijn 3 aanbieders van de mobiele telefonie geïnterviewd, te weten: 2 grote en één kleine. Volgens het Straix-rapport representeert een grote mobiele aanbieder circa 30-40% van de markt, en symboliseert een kleinere mobiele operator circa 15% van de markt.

3.2.2.1 Onbeantwoorde oproepen

Geen van de 3 aanbieders van de mobiele telefonie bewaren de verkeersgegevens betreffende de onbeantwoorde oproepen. Wel is in het Stratix-rapport een indicatie gegeven van de benodigde opslagruimte om de verkeersgegevens met betrekking tot deze gesprekken te bewaren.

[6] Bron: Middensommen 2004 voor defensie burgerpersoneel; schaal 7 : EUR 39.559.

Bij een grote aanbieder van de mobiele telefonie (met circa 30-40% marktaandeel) worden circa 18 miljoen records per dag gegenereerd, waarvan 110 bytes per record worden vastgelegd. Dit leidt tot de dagelijkse registratie van circa 2GB (18 miljoen X 100 bytes) verkeersgegevens.

Voor de bewaartermijn van 12 maanden is ongeveer 0,8TB (12 maanden x 30 dagen x 2GB per dag) opslagruimte noodzakelijk. Naar schatting is circa 0,3TB opslagcapaciteit nodig voor een kleine aanbieder van de mobiele telefonie.

Voor de bewaartermijn van 24 maanden is naar verwachting circa 1,5TB (24 maanden x 30 dagen x 2GB per dag) ruimte nodig om de verkeersgegevens aangaande onbeantwoorde oproepen op te slaan.

3.2.2.2 Uitgaande en binnenkomende gesprekken

De 3 genoemde aanbieders van de mobiele telefonie bewaren de verkeersgegevens betreffende de uitgaande en beantwoorde gesprekken inclusief gratis gesprekken (0800). Twee van deze 3 aanbieders bewaren tevens de binnenkomende gesprekken vanuit andere netwerken. De verkeersgegevens aangaande de binnenkomende en uitgaande gesprekken worden door 2 mobiele aanbieders respectievelijk voor 6 maanden en voor 5 maanden en door de kleine mobiele aanbieder voor 6 maanden bewaard.

De eerste aanbieder van de mobiele telefonie met 30-40% (oftewel circa 35%) marktaandeel bewaart de verkeersgegevens met betrekking tot de uitgaande en binnenkomende gesprekken voor 6 maanden. Naar schatting worden 36 miljoen records per dag gegenereerd, waarvan 130 bytes per record worden opgeslagen. Dit leidt tot de dagelijkse registratie van ongeveer 4,7GB (36 miljoen x 130 bytes) verkeersgegevens. Voor 6 maanden standaardopslag is circa 0,9TB (6 maanden x 30 dagen x 4,7GB per dag) opslagruimte nodig. Uitgaande van het hierboven genoemde marktaandeel heeft de gehele markt circa 103 miljoen (36 miljoen / 35% marktaandeel) gesprekken, waarvan 130 bytes per record worden geregistreerd.

In het Stratix-rapport is aangegeven dat bij de kleine mobiele aanbieder circa 0,4TB opslagruimte nodig is om de verkeersgegevens betreffende de uitgaande en binnenkomende gesprekken 6 maanden langer te bewaren. Een nadere detaillering van deze schatting ontbreekt.

Bij de berekening van de geraamde kosten voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden is de eerste grote aanbieder van de mobiele telefonie met een ruim marktaandeel (circa 30-40%) en met de standaardopslag van 6 maanden als voorbeeld gehanteerd.

De uitbreiding naar 12 maanden houdt in dat de verkeersgegevens 6 maanden langer dan de thans gebruikelijke bewaartermijn dienen te worden opgeslagen. Voor deze extra bewaartermijn is eveneens circa 0,9TB opslagcapaciteit nodig. Bij de tweede aanbieder van de mobiele telefonie met hetzelfde percentage marktaandeel en met 5 maanden standaardopslag is circa 1TB (7 maanden x 30 dagen x 4,7GB per dag) opslagruimte nodig om de verkeersgegevens 7 maanden langer te bewaren. Voor de bewaartermijn van 24 maanden is naar schatting een opslagcapaciteit van circa 2,6TB (12 maanden + 6 maanden x 30 dagen x 4,7GB per dag) nodig.

3.2.2.3 Pre-paidgesprekken

Tengevolge van het Besluit Bijzondere Vergaring Nummergegevens Telecommunicatie worden de verkeersgegevens aangaande de pre-paidgesprekken door alle aanbieders van de mobiele telefonie bewaard. Het volume van deze gegevens is in het Stratix-rapport niet expliciet vermeld. Volgens de wet moeten deze gegevens voor tenminste 3 maanden worden bewaard. Bij dit onderzoek is ervan uitgegaan dat het aangegeven verkeersvolume mede betrekking heeft op de pre-paidgesprekken.

3.2.2.4 Totale opslagcapaciteit bij de gekozen aanbieder

Voor de bewaartermijn van 12 maanden wordt de extra benodigde capaciteit voor de opslag van de onbeantwoorde oproepen, uitgaande en binnenkomende gesprekken, en pre-paidgesprekken geschat op 1,7TB (0,8TB + 0,9TB). Dit betreft 6 maanden extra opslag ten opzichte van de 6 maanden die de mobiele aanbieder nu hanteert.

Voor de bewaartermijn van 24 maanden is circa 4,1TB (1,5TB + 2,6TB) extra opslagruimte noodzakelijk.

3.2.2.5 Investeringskosten

De voor de berekening van de geraamde investeringskosten en exploitatie- en beheerkosten van de vaste telefonie aangereikte argumentatie geldt eveneens voor de mobiele telefoniediensten. Dit houdt voor de eerstgenoemde kostensoort concreet in dat additionele hardware-investeringen nodig zijn om de benodigde verkeersgegevens voor de gewenste bewaartermijnen te bewaren. Een ruwe indicatie conform de prijsopgave van een hardwareleverancier voor een server van een bekend merk met de opslagcapaciteit van circa 1,7TB, en voor een server met een opslagcapaciteit van ongeveer 4,1TB wordt geschat op respectievelijk EUR 23.324 en EUR 31.024. De geraamde investeringskosten zijn in tabel 3 gepresenteerd.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Software licenties	Nihil	Nihil
Hardware	EUR 23.324	EUR 31.024
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-up media	Nihil	Nihil
Uitwijk	Nihil	Nihil
Installatie	Nihil	Nihil
Totaal:	EUR 23.324	EUR 31.024

Tabel 3. Geraamde initiële investeringskosten voor de mobiele telefoniediensten van de aanbieder met 30-40% marktaandeel.

3.2.2.6 Exploitatie- en beheerkosten

Doorgaans kunnen de geraamde exploitatie- en beheerkosten ten behoeve van de opslag als nihil worden beschouwd rekeninghoudend met de hierboven aangereikte argumentatie. Uitgaande van de hierboven gemaakte aanname is er sprake van 70 (1400 verzoeken / 20 dagen) bevragingen per dag. Hierdoor bedragen de personeelskosten circa EUR 80.000 (2 fte's á EUR 40.000) per jaar. Een overzicht van de totale exploitatie- en beheerkosten is in tabel 4 gegeven.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	Nihil	Nihil
- Bevraging	EUR 80.000	EUR 80.000
Inhuur	Nihil	Nihil
Huisvesting	Nihil	Nihil
Huurlijnen	Nihil	Nihil
Totaal:	EUR 80.000	EUR 80.000

Tabel 4. Geraamde jaarlijkse exploitatie- en beheerkosten voor de mobiele telefoniediensten van de aanbieder met 30-40% marktaandeel.

3.2.3 Internettoegang

Voor de internetoegang zijn 6 openbare ISPs verdeeld over kleine, middelgrote en grote organisaties, en één niet-openbare aanbieder genoemd in het kader van het Stratix-onderzoek. Deze ISPs bieden toegang tot internet via huurlijnen, Asymmetric Digital Subscriber Line (ADSL), kabel en inbelfaciliteiten waarmee deze onderzochte aanbieders een goed beeld van de industrie representeren. Vanuit kwantitatief opzicht kan een steekproef van 7 partijen uit een populatie van meer dan honderd ISPs nauwelijks representatief zijn. Alle genoemde ISPs registreren en bewaren verkeersgegevens betreffende de internettoegangssessies, waarvoor de bewaartermijn van enkele dagen tot enkele maanden worden gehanteerd. De kleinste van de onderzochte aanbieders logt als enige ook Internet Protocol (IP)-accounting gegevens (zoals bron, bestemming, volume en datum/tijd). Opgemerkt is dat een deel van de verkeersgegevens verloren gaat als gevolg van het hiervoor gebruikte User Datagram Protocol (UDP)[7] met een relatief beperkte betrouwbaarheid.

3.2.3.1 Toegangsessies

Uitgaande van 6 miljard internetinbelminuten worden ongeveer 150 miljoen toegangsessies gelogd. Deze genereren 300 miljoen records per maand exclusief circa 60 miljoen records per maand voor kabel en ADSL-toegang. In totaal worden 360 miljoen records per maand opgeslagen. De opslag van inlogsessies van een Remote Access Dial In User Service (RADIUS)[8] of Dynamic Host Configuration Protocol (DHCP)[9] log vergt ongeveer 600 bytes per record.

[7] Een berichtgeoriënteerd protocol.
[8] Authenticatieprotocol.
[9] Technisch protocol voor het toekennen van IP-adressen.

Hiermee komt het totale verkeersvolume uit op circa 220GB (360 miljoen x 600 bytes) per maand. Dit houdt ongeveer 22GB (220GB x 10% marktaandeel) verkeersgegevens per maand in voor de grootste ISPs met 10% van de markt, en 1GB á 2GB verkeersgegevens per maand voor een middelgrote aanbieder.

Een aantal ISPs bewaart de verkeersgegevens enkele weken; voor dit onderzoek is van 4 weken (1 maand) uitgegaan. De uitbreiding naar de bewaartermijn van 12 maanden houdt in dat de verkeersgegevens 11 maanden langer dienen te worden bewaard. Er is circa 250GB (11 maanden x 22GB per maand) opslagruimte nodig voor een grote ISP om de verkeersgegevens aangaande de toegangssessies 11 maanden langer te bewaren.

Voor de bewaartermijn van 24 maanden is 510GB (12 maanden + 11 maanden x 22GB per maand) ruimte nodig om de verkeersgegevens met betrekking tot de toegangsessies op te slaan.

3.2.3.2 IP-accounting

De vastlegging van IP-accountinggegevens is van een totaal andere orde dan die met betrekking tot de toegangssessies. De enige in het kader van het Stratix-onderzoek genoemde ISP heeft aangegeven dat, op een datastroom van 2Mbit/seconde, 8 megabyte (MB) per uur IP-accounting gegevens wordt gegenereerd. Met naar schatting 25Gbit/seconde relevant internetverkeer[10] in Nederland is beredeneerd dat de vastlegging van de IP-accounting gegevens in intervallen van 5 minuten, uitkomt op circa 60TB verkeersgegevens per maand. Voor een grote ISP met 10% marktaandeel komt dit naar schatting uit op ongeveer 6TB per maand.

Voor de bewaartermijn van 12 maanden is 72TB (12 maanden x 6TB per maand) opslagruimte nodig om de verkeersgegevens aangaande IP-accounting op te slaan.

Voor de bewaartermijn van 24 maanden is circa 144TB (24 maanden x 6TB per maand) opslagcapaciteit nodig om de verkeersgegevens betreffende IP-accounting op te slaan.

3.2.3.3 Totale opslagcapaciteit bij de gekozen aanbieder

Voor de bewaartermijn van 12 maanden wordt de totale benodigde capaciteit voor de opslag van de gegevens aangaande de toegangsessies en IP-accounting geschat op 73TB (250GB + 72TB), waarbij met enige overhead is rekening gehouden.

Voor de bewaartermijn van 24 maanden is ongeveer 145TB (510GB + 144TB) opslagruimte nodig om de verkeersgegevens op te slaan. Bij deze berekening is rekening gehouden met enige overhead.

[10] Gepubliceerde cijfers van Amsterdam Exchange laten een hogere toename van het internetverkeer zien ten opzichte van het in het Stratix-rapport aangegeven volume.

3.2.3.4 Investeringskosten

Voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden is de berekening van de geraamde investeringskosten en exploitatie- en beheerkosten voor dergelijke uiterst omvangrijke opslagcapaciteiten door het gebrek aan details nauwelijks mogelijk. De hiervoor benodigde hardware is van een totaal andere orde dan een zware server aangevuld met voldoende opslagruimte hetgeen voor de vaste en mobiele telefonie kan worden gebruikt. Voor de opslag van de hierboven geschatte hoeveelheid verkeersgegevens aangaande de toegangssessies en IP-accounting is een geavanceerd opslagmedium nodig waarvoor thans nauwelijks een prijslijst bestaat. In dergelijke gevallen wordt meestal gedacht aan een Storage Area Network (SAN)-oplossing die in feite een snel netwerk is dat het opslagmedium en de servers met elkaar verbindt. De aanschafprijs van dergelijke hardware is afhankelijk van een aantal factoren dat nog niet concreet bekend is, waaronder de te verwachten werklast en de geëiste responsetijd. Mede afhankelijk hiervan worden de softwarelicenties en upgrades overeengekomen. Een ruwe indicatie conform de prijsopgave van een SAN-leverancier voor een hardware met de opslagcapaciteit van 73TB wordt geschat op EUR 1,5 à EUR 2 miljoen. Volgens deze leverancier wordt de hardware-investering voor 145TB geraamd op EUR 2,2 à EUR 3 miljoen.

De installatie van dergelijke opslagmedia heeft normaliter een grote impact op de in gebruik zijnde IT-infrastructuur waarvoor mogelijk applicaties moeten worden gewijzigd, componenten moeten worden vervangen of nieuwe applicaties moeten worden ontwikkeld. Door het gebrek aan inzicht in de infrastructuur van de aanbieder is het lastig de daarbijbehorende kosten te ramen. Daarnaast is in het Stratix-rapport aangegeven dat het bij de internetaanbieder in gebruik zijnde systeem bij voorkeur 5MB per seconde moet aankunnen om tijdens de piektijden de verkeersgegevens te kunnen verwerken. Dit kan mogelijk een aanzienlijke invloed hebben op de door de aanbieder aangelegde infrastructuur waarvan de hiermee gepaard gaande kosten, mede door het gebrek aan inzicht in de daarin opgenomen IT-componenten, niet kunnen worden geschat. De gevolgen van deze veranderingen op de back-up en uitwijk kunnen tevens amper worden bepaald waardoor geen onderbouwde uitspraak kan worden gedaan omtrent de daarmee geassocieerde kosten. Mede door deze onduidelijkheden is voor de investeringskosten alleen de kosten van de aanschaf van de hardware aangegeven.

3.2.3.5 Exploitatie- en beheerkosten

De bovenstaande argumentatie geldt eveneens voor de exploitatie- en beheerkosten aangaande de bewaartermijnen van 12 en 24 maanden. Nadat het benodigde opslagmedium op basis van de eisen en wensen van de behoeftestellers bekend is, kunnen pas de personeelskosten, huisvestingskosten en eventuele kosten van inhuur en huurlijnen worden berekend. In de praktijk blijkt dat de totale exploitatie- en beheerkosten van een omvangrijke opslagcapaciteit met name door 2 componenten wordt beïnvloed, te weten: huisvesting en personeel. Voor het laatstgenoemde is reeds een prijsindictie (schaal 7) gegeven. Circa EUR 1.000 per vierkante meter per jaar wordt in rekening gebracht voor de computervloer.

Wel kan een schatting worden gegeven van de personeelskosten ten behoeve van de bevraging. Uitgaande van de hierboven gemaakte aanname is er sprake van 0,5 (10 verzoeken / 20 dagen) bevragingen per dag.

Ondanks dat hiervoor benodigde inspanning als minimaal kan worden beschouwd, is uitgegaan van ½ fte waarbij met enige groei rekening is gehouden. Hierdoor bedragen de personeelskosten EUR 20.000 (½ fte x EUR 40.000) per jaar. Gezien de ontbrekende gegevens aangaande de resterende kostencomponenten zijn deze ramingen niet in tabelvorm weergegeven.

3.2.4 E-mail

Het hierboven genoemde aantal ISPs is in het kader van het Stratix-onderzoek eveneens genoemd voor de e-maildienst.

3.2.4.1 Post Office Protocol version 3 (POP3) logs

De meeste ISPs leggen verkeersgegevens aangaande POP3 vast voor zover zij deze dienst aanbieden. POP3-logs zijn geregistreerd wanneer gebruikers hun mailbox benaderden, hoeveel berichten zij ophaalden inclusief hun grootte en hoeveel berichten zij lieten staan. Eén ISP bewaart geen POP3-gegevens. Deze aanbieder verwerkt miljoenen POP3-sessies per dag en legt uitsluitend het laatste tijdstip vast dat een gebruiker de mailbox raadpleegde.

Het volume van de verkeersgegevens voor het ophalen van e-mail is substantieel hoger dan dat van de toegangssessies. Aangegeven is dat naar schatting van enkele ISPs 5 à 10 keer zoveel POP3-mailboxloggegevens zijn als gegevens met betrekking tot de toegangssessies per gebruiker. Gebruikers met vaste aansluitingen (zoals kabelmodems en ADSL) hebben vaker de neiging hun mailbox te raadplegen. Dit resulteert in circa 2,5 miljard records van ieder 400 bytes per maand voor alle ISPs hetgeen leidt tot 1TB (2,5 miljard x 400 bytes) verkeersgegevens betreffende POP3. Dit houdt ongeveer 100GB (1TB x 10% marktaandeel) verkeersgegevens per maand in voor de grootste ISPs met 10% marktaandeel.

Voor de bewaartermijn van 12 maanden is een opslagcapaciteit van circa 1,2TB (12 maanden x 100GB per maand) nodig om de POP3-gegevens op te slaan.

Voor de bewaartermijn van 24 maanden is ongeveer 2,4TB (24 maanden x 100GB per maand) opslagruimte noodzakelijk om de POP3-logs te bewaren.

3.2.4.2 Simple Mail Transfer Protocol (SMTP) logs

De meeste ISPs leggen verkeersgegevens betreffende SMTP vast voor zover zij deze dienst aanbieden. In SMTP-logs is per e-mailbericht de afzender, bestemming en datum (en vaak meer gegevens) vastgelegd. Eén ISP beschikt niet over een SMTP-log.

Naast mailboxlogs kunnen ook verkeersgegevens betreffende de individuele berichten (SMTP logs) worden vastgelegd. ISPs blijken deze gegevens in de praktijk te registreren en na een week te overschrijven. Aangegeven is dat een ruwe schatting leert dat het Nederlandse e-mailverkeer ongeveer 60 miljoen records per dag, oftewel 1,8 miljard records per maand van ieder 600 bytes genereert hetgeen resulteert in ongeveer 1,1TB (1,8 miljard x 600bytes) verkeersgegevens aan-

gaande SMTP. Hierbij is met enige overhead rekening gehouden. Dit houdt ongeveer 110GB (1,1TB x 10% marktaandeel) verkeersgegevens per maand in voor de grootste ISPs met 10% marktaandeel.

Voor de bewaartermijn van 12 maanden is een opslagcapaciteit van circa 1,4TB (12 maanden x 110GB per maand) nodig om de SMTP-gegevens op te slaan waarbij met enige overhead rekening is gehouden.

Voor de bewaartermijn van 24 maanden is ongeveer 2,8TB (24 maanden x 110GB per maand) opslagruimte nodig om de SMTP logs te bewaren. Bij deze berekening is rekening gehouden met enige overhead.

3.2.4.3 Totale opslagcapaciteit bij de gekozen aanbieder

Voor de bewaartermijn van 12 maanden wordt de totale benodigde capaciteit voor de opslag van de POP3- en SMTP-logs geschat op 2,6TB (1,2TB + 1,4TB).

Voor de bewaartermijn van 24 maanden is circa 5,2TB (2,4TB + 2,8TB) opslagruimte nodig om de verkeersgegevens op te slaan.

3.2.4.4 Investeringskosten

De voor de berekening van de geraamde investeringskosten en exploitatie- en beheerkosten van de mobiele telefonie aangereikte argumentatie geldt eveneens voor de e-maildiensten. Dit houdt voor de eerstgenoemde kostensoort concreet in dat additionele hardware-investering nodig is om de benodigde verkeersgegevens voor de gewenste bewaartermijnen te bewaren. Een ruwe indicatie conform de prijsopgave van een hardwareleverancier voor een server van een bekend merk met de opslagcapaciteit van circa 2,6TB, en voor een server van een bekend merk met een opslagcapaciteit van ongeveer 5,2TB wordt geschat op respectievelijk EUR 25.524 en EUR 48.618. De geraamde investeringskosten voor de bewaartermijnen van 12 en 24 maanden zijn in tabel 5 gepresenteerd.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	Nihil	Nihil
Hardware	EUR 25.524	EUR 48.618
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	Nihil	Nihil
Uitwijk	Nihil	Nihil
Installatie	Nihil	Nihil
Totaal:	EUR 25.524	EUR 48.618

Tabel 5. Geraamde initiële investeringskosten voor de e-maildiensten van de aanbieder met 10% marktaandeel.

3.2.4.5 Exploitatie- en beheerkosten

Doorgaans kunnen de geraamde exploitatie- en beheerkosten ten behoeve van de opslag als nihil worden beschouwd, gezien de hierboven aangereikte argumentatie. Uitgaande van de hierboven gemaakte aanname is er sprake van 0,5 (10 verzoeken / 20 dagen) bevragingen per dag. Ondanks dat hiervoor benodigde inspanning als minimaal kan worden beschouwd, is uitgegaan van ½ fte waarbij met enige groei rekening is gehouden. Hierdoor bedragen de personeelskosten EUR 20.000 per jaar. Een overzicht van de totale exploitatie- en beheerkosten is in tabel 6 gegeven.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	Nihil	Nihil
- Bevraging	EUR 20.000	EUR 20.000
Inhuur	Nihil	Nihil
Huisvesting	Nihil	Nihil
Huurlijnen	Nihil	Nihil
Totaal:	EUR 20.000	EUR 20.000

Tabel 6. Geraamde jaarlijkse exploitatie- en beheerkosten voor de e-maildiensten van de aanbieder met 10% marktaandeel.

3.2.5 Toegang tot internet via internetcafés

In het Stratix-rapport zijn 2 internetcafés (één kleine en één grote) genoemd.

3.2.5.1 Toegangsessies

Gebleken is dat de 2 genoemde aanbieders relatief weinig informatie vastleggen en de lijst van bezochte websites overschrijven. Kleinere internetcafés hebben momenteel geen noodzaak de verkeersgegevens betreffende de toegangsessies te registreren. De grote aanbieder legt deze gegevens wel vast ten behoeve van de marketingdoeleinden. Nadere detaillering van het verkeersvolume voor de internetcafés is niet gegeven. Aangezien een grote ISP circa 10% van de markt in eigen bezit heeft, is aangenomen dat een groot internetcafé 1% van de markt representeert. Voor deze aanbieder betekent dit circa 2,2GB (220GB x 1% marktaandeel) per maand verkeersgegevens.

Voor de bewaartermijn van 12 maanden is een opslagcapaciteit van ongeveer 27GB (12 maanden x 2,2GB per maand) nodig om verkeersgegevens te bewaren.

Voor de bewaartermijn van 24 maanden is circa 53GB (24 maanden x 2,2GB per maand) opslagruimte is nodig om de verkeersgegevens op te slaan.

3.2.5.2 Totale opslagcapaciteit bij de gekozen aanbieder

De totale benodigde capaciteit voor de opslag van de gegevens aangaande de toegangsessies voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden komt overeen met de hierboven gecalculeerde ruimte.

3.2.5.3 Investeringskosten

Door het gebrek aan inzicht in de bij het grote internetcafé aangelegde infrastructuur is het amper mogelijk de investeringskosten voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden te ramen. Deze kosten zijn derhalve niet in tabelvorm weergegeven. Verwacht wordt dat een bewaarplicht voor lokaal op de PC's opgeslagen verkeersgegevens aanzienlijke impact voor het internetcafé zal hebben aangezien deze aanbieder geen proces heeft geïmplementeerd om deze gegevens te bewaren. Dit houdt in dat het internetcafé zowel het netwerk als de bedrijfsvoering anders dient in te richten teneinde de verkeersgegevens vast te kunnen leggen. Lokale PC's en de bijbehorende software moeten daardoor mogelijk worden aangepast alsmede de in gebruik zijnde server en de daarop draaiende software, waarna deze nieuwe configuratie wordt geïnstalleerd. De prijs van een voor het internetcafé relevante PC van een bekend merk varieert thans van circa EUR 500 tot EUR 1.500. Een ruwe indicatie conform de prijsopgave van een hardleverancier voor een server met de opslagcapaciteit van 27GB met de uitbreidingsmogelijkheid tot 145GB wordt geschat op EUR 2.730. Geen informatie omtrent de uitwijk bij het internetcafé is gegeven, waardoor is verondersteld dat dit aspect minder relevant is voor deze aanbieder. Voor de beschikbaarstelling van de verkeersgegevens dient de back-up op een adequate wijze door het internetcafé te worden geregeld. Gezien het te bewaren verkeersvolume kunnen de daarbijbehorende kosten pas na een impactanalyse worden geraamd.

3.2.5.4 Exploitatie- en beheerkosten

Aangezien deze aanbieder reeds voor de huisvesting betaalt, is ervan uitgegaan dat de wijzigingen in de infrastructuur nauwelijks additionele fysieke ruimte vergen, aangezien in de huidige situatie al rekening is gehouden met de benodigde ruimte voor de apparatuur. De geschatte exploitatie- en beheerkosten zijn in tabel 7 gepresenteerd. Uitgaande van de hierboven gemaakte aanname is er sprake van 0,5 (10 verzoeken / 20 dagen) bevragingen per dag. Ondanks dat hiervoor benodigde inspanning als minimaal kan worden beschouwd, is uitgegaan van 0,2 fte waarbij met enige groei rekening is gehouden. Hierdoor bedragen de personeelskosten EUR 8.000.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	EUR 4.000	EUR 4.000
- Bevraging	EUR 4.000	EUR 4.000
Inhuur	Nihil	Nihil
Huisvesting	Nihil	Nihil
Huurlijnen	Nihil	Nihil
Totaal:	EUR 8.000	EUR 8.000

Tabel 7. Geraamde jaarlijkse exploitatie- en beheerkosten voor de toegang tot internet via internetcafé met 1% marktaandeel.

3.3 Optie 2: opslag en bevraging bij de overheid

Per telecommunicatiedienst is de berekening van de geraamde investerings-, exploitatie- en beheerkosten in de volgende secties beschreven. Als input voor deze calculatie zijn onder meer de reeds hierboven uitgerekende opslagruimte gebruikt. Tevens zijn de door de overheidsinstantie aangereikte prijzen meegenomen in de berekening van de investeringskosten alsmede exploitatie- en beheerkosten van deze optie. Voor het laatstgenoemde is een nieuw kostencomponent toegevoegd, te weten: vergoedingen. Deze component representeert de jaarlijkse vergoedingen aan alle aanbieders voor het aanleveren van gegevens aan de overheidsinstantie.

3.3.1 Vaste telefonie

Door de gehele markt wordt naar verwachting circa 50 miljoen records betreffende de uitgaande gesprekken per dag gegenereerd, zoals hierboven aangegeven. Hiervan worden 110 bytes per record vastgelegd. Dit leidt tot de dagelijkse registratie van 5,5GB (50 miljoen x 110 bytes) verkeersgegevens.

3.3.1.1 Totale opslagcapaciteit bij de overheid

Voor de bewaartermijn van 12 maanden is naar verwachting ongeveer 2TB (12 maanden x 30 dagen x 5,5GB per dag) ruimte nodig om de verkeersgegevens op te slaan.

Voor de bewaartermijn van 24 maanden is circa 4TB (24 maanden x 30 dagen x 5,5GB per dag) opslagcapaciteit noodzakelijk om de verkeersgegevens te bewaren.

3.3.1.2 Investeringskosten

Zoals in tabel 8 aangegeven wordt de totale geraamde investeringskosten voor 2TB geschat op EUR 286.893. Ten behoeve van deze opslagcapaciteit zijn er softwarelicenties nodig voor de

databaseserver waarvan de kosten EUR 1.520 bedragen conform het contract tussen het Ministerie van Justitie en Microsoft. Hierbij is uitgegaan van Windows Server (EUR 789) en SQL Server (EUR 731) waarvoor minder dan 4 processoren zijn gebruikt. Tevens is aangenomen dat met upgrades gepaard gaande kosten onderdeel uitmaken van het contract. Voor de hardware van een bekend merk met 2TB opslagcapaciteit wordt EUR 22.640 in rekening gebracht. Aangezien de gegevens volgens het bij de overheidsinstantie in gebruik zijnde concept door de aanbieders worden aangeleverd, is verondersteld dat de bestaande applicaties niet worden aangepast, geen uitwijk hoeft te worden geregeld en geen nieuwe applicaties worden ontwikkeld. De functionaliteit van de overheidsinstantie dient wel te worden uitgebreid, zodat de verkeersgegevens bevraagbaar worden gemaakt. Hiervoor worden de applicaties eenmalig aangepast waarvan de kosten naar schatting circa EUR 250.000 bedragen. De prijsopgave van een adequate back-upmedia bedraagt EUR 11.533 hetgeen op tapes is gebaseerd. Voor de installatie van een dergelijke opslagcapaciteit wordt 3 dagen inspanning gerekend die naar schatting circa EUR 1.200 (3 dagen x EUR 400) kost.

De totale geraamde investeringskosten voor 4TB wordt geschat op EUR 305.560, zoals in tabel 8 getoond. Indien de database groter wordt dan 2TB, wordt de licentieprijs vertienvoudigd. Dit houdt in dat de licentiekosten EUR 7.797 (EUR 789 voor Windows + EUR 7.008 voor SQL Server) bedragen rekeninghoudend met de omvang van de database. Voor de hardware van een bekend merk met een opslagcapaciteit van 4TB wordt EUR 34.630 in rekening gebracht. De ten behoeve van de bewaartermijn van 12 maanden aangereikte argumentaties voor de wijziging applicaties, nieuwe applicaties, upgrades en uitwijk gelden eveneens voor de bewaartermijn van 24 maanden. Tevens is aangenomen dat de back-upmedia met marginale kosten voor de opslagcapaciteit van 4TB kan worden gebruikt. Voor de installatie wordt naar schatting een inspanning van 4 dagen verwacht hetgeen circa EUR 1.600 (4 x EUR 400) kost. Bij de bewaartermijn van 12 maanden is reeds rekening gehouden met de eenmalige kosten die gepaard gaan met de wijziging van applicaties ten behoeve van de bevraging.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	EUR 1.520	EUR 7.797
Hardware	EUR 22.640	EUR 34.630
Wijziging applicaties:		
- Opslag	Nihil	Nihil
- Bevraging	EUR 250.000	EUR 250.000
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	EUR 11.533	EUR 11.533
Uitwijk	Nihil	Nihil
Installatie	EUR 1.200	EUR 1.600
Totaal:	EUR 286.893	EUR 305.560

Tabel 8. Totale geraamde initiële investeringskosten voor de vaste telefoniediensten.

3.3.1.3 Exploitatie- en beheerkosten

Voor de exploitatie- en beheerkosten ten behoeve van de bewaartermijn van 12 maanden en bewaartermijn van 24 maanden is verondersteld dat 1 fte voor het beheer van ongeveer 2TB verkeersgegevens nodig is. Hierbij is schaal 7 als uitgangpunt gehanteerd met de bijbehorende integrale jaarlijkse kosten, zoals hierboven is aangegeven. Aangenomen is dat circa 10 vierkante meter computervloer nodig is voor ongeveer 2TB opslagcapaciteit met de bijbehorende prijs, zoals reeds genoemd. Verder is verondersteld dat geen inhuur voor het beheer van de opslagcapaciteit plaatsvindt. Momenteel betaalt de overheidsinstantie circa EUR 17.000 per jaar voor de huurlijnen hetgeen in het jaarlijkse budget wordt opgenomen. Voor de berekening van de kosten voor de huurlijnen is aangenomen dat de capaciteit van deze lijnen op jaarbasis wordt verdubbeld bij verkeersvolume groter dan 4TB. De overheidsinstantie betaalt jaarlijks EUR 300.000 aan de aanbieders voor de aanlevering van gegevens.

Ten behoeve van de bevraging bedragen de kosten van het correctief (storingen oplossen) en adaptief onderhoud (aanpassingen op basis van wijzigingen) naar verwachting EUR 50.000 per jaar. De met de huurlijnen geassocieerde kosten voor de bevraging bedragen circa EUR 22.000 per jaar.

Voor de bewaartermijn van 12 maanden bedragen de personeelskosten circa EUR 40.000 per jaar. De huisvesting voor deze bewaartermijn kost respectievelijk EUR 10.000 (10 vierkante meter x EUR 1.000).

Voor de bewaartermijn van 24 maanden bedragen de personeelskosten ongeveer EUR 80.000 (2 x EUR 40.000) per jaar. De huisvesting voor deze bewaartermijn kost EUR 20.000 (20 vierkante meter x EUR 1.000).

Tabel 9 geeft een totaal overzicht van de geraamde exploitatie- en beheerkosten van de vaste telefonie voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	EUR 40.000	EUR 80.000
- Bevraging	EUR 50.000	EUR 50.000
Inhuur	Nihil	Nihil
Huisvesting	EUR 10.000	EUR 20.000
Huurlijnen:		
- Opslag	Nihil	EUR Nihil
- Bevraging	EUR 22.000	EUR 22.000
Vergoedingen	EUR 300.000	EUR 300.000
Totaal:	EUR 422.000	EUR 472.000

Tabel 9. Totale geraamde jaarlijkse exploitatie- en beheerkosten voor de vaste telefoniediensten.

3.3.2 Mobiele telefonie

Door de totale markt worden naar schatting 103 miljoen records met betrekking tot de uitgaande gesprekken per dag gegenereerd, zoals hierboven aangegeven. Hiervan worden 130 bytes per record vastgelegd. Dit resulteert in de dagelijkse registratie van circa 14GB (103 miljoen x 130 bytes) verkeersgegevens.

3.3.2.1 Totale opslagcapaciteit bij de overheid

Voor de bewaartermijn van 12 maanden is naar verwachting ongeveer 5,1TB (12 maanden x 30 dagen x 14GB per dag) ruimte nodig om de uitgaande gesprekken op te slaan. Hierbij wordt tevens de benodigde capaciteit voor de opslag van de onbeantwoorde oproepen opgeteld. Hiermee wordt de totale overheidsopslag geschat op 6TB (5,1TB + 750GB).

Voor de bewaartermijn van 24 maanden is naar schatting circa 10,1TB (24 maanden x 30 dagen x 14GB per dag) opslagcapaciteit noodzakelijk om de verkeersgegevens betreffende de uitgaande gesprekken te bewaren. Hierbij wordt eveneens de benodigde ruimte voor de opslag van de onbeantwoorde oproepen opgeteld. Hiermee wordt de totale overheidsopslag geraamd op 12TB (10,1TB + 1,5TB).

3.3.2.2 Investeringskosten

Zoals in tabel 10 getoond wordt de totale geraamde investeringskosten voor 6TB geschat op EUR 93.085. Gezien de omvang van de database en het aantal in te zetten servers bedragen de licentiekosten EUR 15.594 (2 servers x EUR 7.797). De met de hardware- en back-upgeassocieerde kosten bedragen respectievelijk ongeveer EUR 63.958 en EUR 11.533. Voor de installatie wordt naar schatting een inspanning van 5 dagen verwacht hetgeen circa EUR 2.000,- (5 x EUR 400) kost. De met de bevraging gepaard gaande kosten zijn reeds bij de vaste telefonie meegenomen.

De totale geraamde investeringskosten voor 12TB wordt geschat op EUR 154.347, waarbij is aangenomen dat 3 servers zullen worden gebruikt. De softwarelicenties voor dit opslagvolume bedragen EUR 23.391 (3 x EUR 7.797,-) aangezien de servers in totaal circa EUR 103.890 kosten. De back-up- en installatiekosten worden verdubbeld voor de opslagcapaciteit groter dan 12TB. Deze bedragen respectievelijk EUR 23.066 (2 x EUR 11.533) en EUR 4.000 (10 dagen x EUR 400). Dezelfde beredenering als voor de vaste telefonie geldt voor de resterende kostencomponenten. De kosten van de bevraging zijn reeds meegenomen bij de kosten van de vaste telefoniediensten.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	EUR 15.594	EUR 23.391
Hardware	EUR 63.958	EUR 103.890
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	EUR 11.533	EUR 23.066
Uitwijk	Nihil	Nihil
Installatie	EUR 2.000	EUR 4.000
Totaal:	EUR 93.085	EUR 154.347

Tabel 10. Totale geraamde initiële investeringskosten voor de mobiele telefoniediensten.

3.3.2.3 Exploitatie- en beheerkosten

Ten behoeve van de exploitatie- en beheerkosten van de bewaartermijnen van 12 en 24 maanden zijn dezelfde aannames gehanteerd als voor de vaste telefonie, zoals hierboven uiteengezet. Uitgaande van de hierboven gemaakte aanname bedragen de kosten voor de huurlijnen EUR 17.000 per jaar. De met de bevraging gepaard gaande kosten zijn reeds bij de vaste telefonie meegerekend.

Voor de bewaartermijn van 12 maanden bedragen de personeelskosten EUR 120.000 (3 x EUR 40.000). De huisvesting voor deze bewaartermijn kost EUR 30.000 (30 vierkante meter x EUR 1.000).

Voor de bewaartermijn van 24 maanden bedragen de personeelskosten EUR 240.000,- (6 x EUR 40.000). De huisvesting voor deze bewaartermijn kost EUR 60.000,- (60 vierkante meter x EUR 1.000).

Tabel 11 presenteert de totale geschatte exploitatie- en beheerkosten voor de bewaartermijnen van 12 en 24 maanden.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel	EUR 120.000	EUR 240.000
Inhuur	Nihil	Nihil
Huisvesting	EUR 30.000	EUR 60.000
Huurlijnen	EUR 17.000	EUR 17.000
Vergoedingen	Nihil	Nihil
Totaal:	EUR 167.000	EUR 317.000

Tabel 11. Totale geraamde jaarlijkse exploitatie- en beheerkosten voor de mobiele telefoniediensten.

3.3.3 Internettoegang

De hierboven gecalculeerde ruimte voor de opslag van de verkeersgegevens betreffende de internettoegang (toegangssessies en IP-accounting) is voor de bewaartermijnen van 12 en 24 maanden respectievelijk geschat op 73TB en 146TB. Zoals reeds benadrukt hebben deze schattingen betrekking op één grote ISP met 10% marktaandeel die in het kader van het Stratix-onderzoek is genoemd.

3.3.3.1 Totale opslagcapaciteit bij de overheid

Voor de bewaartermijn van 12 maanden is naar verwachting ongeveer 730TB (73TB x 100 / 10) ruimte nodig om de verkeersgegevens aangaande de internettoegang op te slaan.

Voor de bewaartermijn van 24 maanden is naar schatting circa 1,5 petabyte (PB) opslagcapaciteit (146TB x 100 / 10) noodzakelijk om de verkeersgegevens te bewaren.

3.3.3.2 Investeringskosten

Hierboven is een ruwe indicatie gegeven van een mogelijke implementatie volgens het SAN-concept voor dergelijke omvangrijke opslagcapaciteiten. Verder is beargumenteerd dat de schatting van de resterende componenten van de investeringskosten afhankelijk is van een aantal factoren dat nog niet is geconcretiseerd, hetgeen tevens op de exploitatie- en beheerkosten van invloed is. Voorbeelden hiervan zijn de gewenste responsetijd die de keuze van het SAN-concept kunnen beïnvloeden, en de hiervoor benodigde hardware en andere apparatuur die mogelijk een nieuwe huisvesting vergen. Het gebruik van dergelijke opslagsystemen hebben een aanzienlijke impact op de infrastructuur waarvan de consequenties in eerste instantie voor de overheidsinstantie dienen te worden onderzocht. Gezien het ongebruikelijke grote volume is voor deze opslagruimte en verwerkingscapaciteit informatie opgevraagd bij een ICT-service provider die diensten biedt aan de overheidsector. Volgens deze leverancier bedragen de investeringskosten voor een opslagruimte van 730TB circa EUR 7 miljoen per jaar.

De geschatte investeringskosten voor 1,5PB zullen naar verwachting EUR 10 miljoen bedragen.

3.3.3.3 Exploitatie- en beheerkosten

Volgens de in de overheidsector opererende leverancier bedragen de exploitatie- en beheerkosten voor 730TB ongeveer EUR 1 miljoen per jaar, en voor 1,5PB ongeveer EUR 1,5 miljoen per jaar.

3.3.4 E-mail

De hierboven berekende ruimte voor de opslag van de verkeersgegevens betreffende de e-maildiensten is voor de bewaartermijnen van 12 en 24 maanden respectievelijk geschat op 2,6TB en 5,2TB. Zoals reeds aangegeven betreffen deze schattingen één grote ISP met circa 10% marktaandeel die in het kader van het Stratix-onderzoek is genoemd.

3.3.4.1 Totale opslagcapaciteit bij de overheid

Voor de bewaartermijn van 12 maanden is naar schatting circa 26TB (2,6TB x 100 / 10) ruimte nodig om de verkeersgegevens betreffende de e-maildienst op te slaan.

Voor de bewaartermijn van 24 maanden is naar verwachting ongeveer 52TB (5,2TB x 100 / 10) opslagcapaciteit nodig om de verkeersgegevens te bewaren.

3.3.4.2 Investeringskosten

Voor de bewaartermijn van 12 maanden bedragen de geraamde kosten van de hierboven berekende opslagcapaciteit van 26TB naar schatting circa EUR 260.000.

Voor de bewaartermijn van 24 maanden zullen de geschatte kosten voor de opslag van 52TB naar schatting EUR 520.000 miljoen bedragen.

3.3.4.3 Exploitatie- en beheerkosten

Voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden zijn de geschatte kosten van de hierboven berekende opslagcapaciteit door gebrek aan gedetailleerde informatie moeilijk te bepalen, aangezien de eisen van de behoeftestellers niet zijn gedocumenteerd. In het kader van dit onderzoek worden de kosten van de huisvesting en het personeel respectievelijk op EUR 100.000 en EUR 150.000 geschat.

3.3.5 Toegang tot internet via internetcafés

De hierboven gecalculeerde ruimte voor de opslag van de verkeersgegevens met betrekking tot de toegang tot internet via internetcafés is voor de bewaartermijnen van 12 en 24 maanden respectievelijk geschat op 27GB en 55GB. Zoals reeds aangegeven betreffen deze schattingen één groot internetcafé met circa 1% marktaandeel die in het kader van het Stratix-onderzoek is genoemd.

3.3.5.1 Totale opslagcapaciteit bij de overheid

Voor de bewaartermijn van 12 maanden is naar verwachting ongeveer 2,7TB (27GB x 100) ruimte nodig om de verkeersgegevens betreffende de toegang tot internet via internetcafés op te slaan.

Ten behoeve van de bewaartermijn van 24 maanden is naar schatting circa 5,5TB (55GB x 100) opslagcapaciteit nodig om de verkeersgegevens te bewaren.

3.3.5.2 Investeringskosten

De investeringskosten voor een opslagcapaciteit van 2,7TB worden geraamd op EUR 49.354. De argumentatie hiervoor is hierboven reeds aan de orde geweest. Aangezien deze ruimte nagenoeg vergelijkbaar is met de benodigde opslagcapaciteit voor de vaste telefonie (3TB), is de hiervoor geschatte prijs voor hardware gehanteerd.

De investeringskosten voor een opslagcapaciteit van 5,5TB worden geraamd op EUR 93.085. Aangezien deze ruimte nagenoeg vergelijkbaar is met de benodigde opslagcapaciteit voor de mobiele telefonie (6TB), zijn de hiervoor geraamde investeringskosten gehanteerd.

Een overzicht van de investeringskosten voor de bewaartermijnen 12 en 24 maanden is in tabel 12 gegeven.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	EUR 7.797	EUR 15.594
Hardware	EUR 28. 824	EUR 63.958
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	EUR 11.533	EUR 11.533
Uitwijk	Nihil	Nihil
Installatie	EUR 1.200	EUR 2.000
Totaal:	EUR 49.354	EUR 93.085

Tabel 12. Totale geraamde initiële investeringskosten voor de toegang tot internet via internetcafés.

3.3.5.3 Exploitatie- en beheerkosten

De exploitatie- en beheerkosten voor 2,7TB wordt geschat op EUR 50.000.

De exploitatie- en beheerkosten voor 5,5TB wordt geschat op EUR 100.000. De argumentatie hiervoor is hierboven eveneens toegelicht.

Een overzicht van de investeringskosten voor de bewaartermijnen 12 en 24 maanden is in tabel 13 gepresenteerd.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel	EUR 40.000	EUR 80.000
Inhuur	Nihil	Nihil
Huisvesting	EUR 10.000	EUR 20.000
Huurlijnen	Nihil	Nihil
Vergoedingen	Nihil	Nihil
Totaal:	EUR 50.000	EUR 100.000

Tabel 13. Totale geraamde jaarlijkse exploitatie- en beheerkosten voor de toegang tot internet via internetcafés.

3.4 Totaal kostenoverzicht

Het totale overzicht van de geraamde kosten van optie 1 en optie 2 is respectievelijk in de tabel 14 en tabel 15 gepresenteerd. Hierbij zijn de uitgangspunten betreffende de bewaartermijn van 12 maanden en de bewaartermijn van 24 maanden in acht genomen. De totstandkoming van deze kosten is hierboven separaat uiteengezet.

Optie 1 voor gekozen aanbieder	**Marktaandeel**	**Bewaartermijn 12 maanden**	**Bewaartermijn 24 maanden**
Initiële investeringskosten:			
Vaste telefonie	70%	EUR 18.144	EUR 28.824
Mobiele telefonie	30-40%	EUR 23.324	EUR 31.024
Internettoegang	10%	EUR 1,5 - EUR 2 miljoen	EUR 2,2 - EUR 3 miljoen
E-mail	10%	EUR 25.524	EUR 48.618
Toegang tot internet via internetcafés	1%	EUR 2.730	EUR 2.730
Jaarlijkse exploitatie- en beheerkosten:			
Vaste telefonie	70%	EUR 40.000	EUR 40.000
Mobiele telefonie	30-40%	EUR 80.000	EUR 80.000
Internettoegang:	10%		
- Personeel bevraging		EUR 20.000	EUR 20.000
E-mail:	10%		
- Personeel bevraging		EUR 20.000	EUR 20.000
Toegang tot internet via internetcafés	1%	EUR 8.000	EUR 8.000

Tabel 14. Overzicht geraamde kosten van optie 1.

Optie 2 gesommeerd voor overheid	**Bewaartermijn 12 maanden**	**Bewaartermijn 24 maanden**
Initiële investeringskosten:		
Vaste telefonie	EUR 286.893	EUR 305.560
Mobiele telefonie	EUR 93.085	EUR 154.347
Internettoegang	EUR 7 miljoen	EUR 10 miljoen
E-mail	EUR 260.000	EUR 520.000
Toegang tot internet via internetcafés	EUR 49.354	EUR 93.085
Jaarlijkse exploitatie- en beheerkosten:		
Vaste telefonie	EUR 422.000	EUR 472.000
Mobiele telefonie	EUR 167.000	EUR 317.000
Internettoegang	EUR 1 miljoen	EUR 1,5 miljoen
E-mail	EUR 100.000	EUR 150.000
Toegang tot internet via internetcafés	EUR 50.000	EUR 100.000

Tabel 15. Overzicht geschatte kosten van optie 2.

3.5 Consequenties toename telecommunicatieverkeer

In 2003 heeft het verkeersvolume aangaande de vaste telefonie de teruglopende trend gecontinueerd. Hoofdzakelijk is deze afname mede veroorzaakt door de groei van de mobiele telefonie en het expanderende gebruik van breedbandinternettoegang. Het aantal mobiele telefonieabonnees steeg in 2003, voornamelijk door een toename van het aantal abonnees van de kleinere mobiele aanbieders. Het internetgebruik ligt op een hoog niveau in Nederland. In 2003 is het aantal breedbandinternetaansluitingen sterk gegroeid.[11]

De in het Stratix-rapport beschreven telecommunicatiediensten zijn in deze fase in 2 categorieën verdeeld. De eerste categorie bevat vaste en mobiele telefoniediensten en wordt hierna telecomverkeer genoemd. De aanbieder hiervan wordt in deze fase aangeduid als telefonieaanbieder. Internettoegang, e-mail en toegang tot internet via internetcafés zijn onderdeel van de tweede categorie waaraan als internetverkeer wordt gerefereerd. De aanbieder hiervan wordt in deze fase aangeduid als ISP. Op basis van de onderzoekvraagstelling is uitgegaan van een toename van het telecomverkeer met 25%. Zoals gevraagd is in deze fase rekening gehouden met de explosieve groei van het internetverkeer. Hiervoor is derhalve uitgegaan van een stijging met 100%. Ten behoeve van het telecom- en internetverkeer zijn de hierboven geschatte verkeersvolumes als input gebruikt. Deze schattingen zijn gebaseerd op de volumegegevens die in het Stratix-rapport zijn opgenomen.

3.5.1 Optie 1

In deze sectie zijn de organisatorische en technische gevolgen van de groei van het telecom- en internetverkeer separaat beschreven. Een indicatie van de financiële consequenties van deze stijging is tevens gegeven.

3.5.1.1 Telecomverkeer: vaste telefonie

De organisatorische en technische gevolgen van de stijging van het vaste telefonieverkeer tezamen met een schatting van de bijbehorende kosten zijn hieronder uiteengezet.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het telecomverkeer met 25% in ongeveer 0,3TB (1,2TB[12] x 25%) additionele opslagcapaciteit.

[11] Bron: TNO Strategie, Technologie en Beleid, Netwerken in cijfers 2004: Trendrapportage ICT-infrastructuur en diensten, 9 juni 2004.
[12] Geschatte opslagcapaciteit voor de vaste telefonie zoals hierboven berekend.

Voor de bewaartermijn van 24 maanden leidt de stijging van het telecomverkeer met 25% tot circa 0,8TB (3TB[13] x 25%) bijkomende opslagruimte.

De verwachting is dat het met geheel geen of minimale wijzigingen mogelijk is deze relatief lichte opslagtoename aan te kunnen. De geïmplementeerde organisatorische vergaar-, opslag- en verstrekkingprocedures bij de telefonieaanbieder met 70% marktaandeel behoeven derhalve nauwelijks veranderingen. Hierbij is rekening gehouden met de ervaring van de telefonieaanbieders waar het gaat om de coöperatie met de behoeftestellers, alsmede met de wet- en regelgeving. Organisatorische veranderingen zijn reeds door deze aanbieders doorgevoerd teneinde een optimale bevraging mogelijk te maken, zodat onverwijld kan worden gereageerd. Dit houdt concreet in dat de telefonieaanbieder procedures heeft geïmplementeerd om de door de behoeftestellers te initiëren verzoeken en vorderingen in ontvangst te nemen en verder af te handelen. Daarom kunnen de organisatorische consequenties voor het opslaan van de historische verkeersgegevens bij de toename van het telecomverkeer met 25% doorgaans als marginaal worden beschouwd. Hierbij is onder andere het artikel 3 van Algemene Inrichtingseisen van de 'Regeling aftappen openbare telecommunicatienetwerken en -diensten' in acht genomen.

Technische consequenties

De technische consequenties van de verkeerstoename met 25% kunnen als marginaal worden beschouwd. Rekeninghoudend met de extra opslag, zoals hierboven berekend, is er hoofdzakelijk sprake van extra hardware.

Investeringskosten

Voor de bewaartermijn van 12 maanden zijn er ongeveer 3 extra harde schijven nodig. Hiermee zullen de totale hardwarekosten naar schatting EUR 19.794 bedragen.

Voor de bewaartermijn van 24 maanden is eveneens additionele hardware noodzakelijk. Hiervan zullen de totale kosten naar verwachting op circa EUR 31.024 uitkomen.

De investeringskosten voor de beide termijnen bij de volumestijging met 25% zijn in tabel 16 weergegeven.

[13] Geraamde opslagruimte voor de vaste telefonie zoals hierboven gecalculeerd.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	Nihil	Nihil
Hardware	EUR 19.794	EUR 31.024
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	Nihil	Nihil
Uitwijk	Nihil	Nihil
Installatie	Nihil	Nihil
Totaal:	EUR 19.794	EUR 31.024

Tabel 16. Geraamde totale investeringskosten voor het vaste telefonieverkeer van de aanbieder met 70% marktaandeel bij de volumetoename met 25%.

Exploitatie- en beheerkosten

Voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden gelden eveneens de hierboven aangereikte argumentaties voor de vaste telefonie. Een overzicht van de bijbehorende exploitatie- en beheerkosten is in tabel 17 getoond.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	Nihil	Nihil
- Bevraging	EUR 40.000	EUR 40.000
Inhuur	Nihil	Nihil
Huisvesting	Nihil	Nihil
Huurlijnen	Nihil	Nihil
Totaal:	EUR 40.000	EUR 40.000

Tabel 17. Geschatte totale exploitatie- en beheerkosten van het vaste telefonieverkeer van de aanbieder met 70% marktaandeel bij de volumestijging met 25%.

3.5.1.2 Telecomverkeer: mobiele telefonie

De organisatorische en technische gevolgen van de toename van het mobiele telefonieverkeer tezamen met een raming van de gepaard gaande kosten zijn hieronder beschreven.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het telecomverkeer met 25% in ongeveer 0,5TB (2TB[14] x 25%) additionele opslagcapaciteit.

Voor de bewaartermijn van 24 maanden leidt de stijging van het telecomverkeer met 25% tot circa 1,1TB (4,1TB[15] x 25%) bijkomende opslagruimte. Hierbij is met enige overhead rekening gehouden.

De hierboven aangereikte argumentatie voor de vaste telefonie is eveneens van toepassing op de mobiele telefonie. Bij de telefonieaanbieder met 30-40% marktaandeel kunnen de organisatorische veranderingen ten behoeve van de opslag van de historische verkeersgegevens bij de stijging van het telecomverkeer met 25% derhalve als beperkt worden beschouwd.

Technische consequenties

De hierboven uitgelegde impact geldt tevens voor de technische consequenties van de verkeerstoename met 25%. Hierboven zijn de technische aspecten onder meer uitvoering aan de orde geweest. Verwacht wordt dat er voornamelijk sprake is van een additionele hardware die onder andere is geëquipeerd met de hierboven gecalculeerde opslagcapaciteit.

Investeringskosten

Voor de bewaartermijn van 12 maanden is een server met de berekende opslagruimte noodzakelijk die naar schatting circa EUR 25.524 kost.

Voor de bewaartermijn van 24 maanden is een machine nodig met de gecalculeerde harde schijf die naar verwachting ongeveer EUR 48.618 kost.

De investeringskosten voor de bovenstaande bewaartermijnen bij de volumetoename met 25% zijn in tabel 18 gepresenteerd.

[14] Geraamde opslagcapaciteit voor de mobiele telefonie zoals hierboven gecalculeerd.
[15] Geschatte opslagruimte voor de mobiele telefonie zoals hierboven gecalculeerd.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	Nihil	Nihil
Hardware	EUR 25.524	EUR 48.618
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	Nihil	Nihil
Uitwijk	Nihil	Nihil
Installatie	Nihil	Nihil
Totaal:	EUR 25.524	EUR 48.618

Tabel 18. Geraamde totale investeringskosten voor het mobiele telefonieverkeer van de aanbieder met 30-40% marktaandeel bij de volumetoename met 25%.

Exploitatie- en beheerkosten

Voor de bewaartermijn van 12 maanden en voor de bewaartermijn van 24 maanden gelden eveneens de hierboven aangereikte argumentatie voor de mobiele telefonie. Een overzicht van de daarbijbehorende exploitatie- en beheerkosten is in tabel 19 gegeven.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	Nihil	Nihil
- Bevraging	EUR 80.000	EUR 80.000
Inhuur	Nihil	Nihil
Huisvesting	Nihil	Nihil
Huurlijnen	Nihil	Nihil
Totaal:	EUR 80.000	EUR 80.000

Tabel 19. Geschatte additionele exploitatie- en beheerkosten voor het mobiele telefonieverkeer van de aanbieder met 30-40% marktaandeel bij de volumestijging met 25%.

3.5.1.3 Internetverkeer: internettoegang

De organisatorische en technische gevolgen van de toename van het verkeer betreffende de internettoegang tezamen met een schatting van de bijbehorende kosten zijn hieronder uiteengezet.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het internetverkeer met 100% bij een grote ISP met 10% marktaandeel in ongeveer 150TB (73TB[16] x 2) additionele opslagcapaciteit.

Voor de bewaartermijn van 24 maanden leidt de stijging van het internetverkeer met 100% bij de ISP met 10% marktaandeel tot circa 300TB (146TB[17] x 2) bijkomende opslagruimte.

Investeringskosten

De opslag van 150TB voor een periode van 12 maanden wordt door een leverancier op een investering van EUR 2,2 à 3 miljoen geschat. Voor de opslag van 300TB voor 24 maanden is dit EUR 3 à 4 miljoen.

Exploitatie- en beheerkosten

De kosten voor de huisvesting zijn in dit stadium nog niet te kwantificeren. Voor personele kosten voor het afhandelen van de bevraging wordt uitgegaan van 0,5 fte, hetgeen EUR 20.000 op jaarbasis inhoudt.

3.5.1.4 Internetverkeer: e-mail

De organisatorische en technische gevolgen van de toename van het verkeer met betrekking tot de e-maildienst tezamen met een raming van de geassocieerde kosten zijn hieronder besproken.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het internetverkeer met 100% bij een grote ISP met 10% marktaandeel in ongeveer 5,5TB (2,6TB[18] x 2) additionele opslagcapaciteit.

Voor de bewaartermijn van 24 maanden leidt de stijging van het internetverkeer met 100% bij een grote ISP met 10% marktaandeel tot circa 11TB (5,2TB[19] x 2) bijkomende opslagruimte.

Investeringskosten

De opslag van 5,5TB voor een periode van 12 maanden wordt geschat op een investering van EUR 48.618. Voor de opslag van 11TB voor een periode van 24 maanden is dit EUR 97.236.

[16] Geschatte opslagcapaciteit voor de internettoegang zoals hierboven berekend.
[17] Geraamde opslagruimte voor de internettoegang zoals hierboven gecalculeerd.
[18] Geraamde opslagruimte voor de e-mail zoals hierboven gecalculeerd.
[19] Geschatte opslagcapaciteit voor de e-mail zoals hierboven berekend.

Exploitatie- en beheerkosten

De kosten voor de huisvesting zijn voor dit volume redelijk beperkt. Voor personeelskosten voor het afhandelen van de bevraging wordt uitgegaan van 0,5 fte, hetgeen EUR 20.000 op jaarbasis inhoudt.

3.5.1.5 Internetverkeer: internetcafé

De organisatorische en technische gevolgen van de toename van het verkeer aangaande de toegang tot internet via internetcafé tezamen met een schatting van de gerelateerde kosten zijn hieronder beschreven.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het internetverkeer met 100% bij een groot internetcafé met 1% marktaandeel in ongeveer 55GB (27GB[20] x 2) additionele opslagcapaciteit.

Voor de bewaartermijn van 24 maanden leidt de stijging van het internetverkeer met 100% bij een groot internetcafé met 1% marktaandeel tot circa 110GB (55GB[21] x 2) bijkomende opslagruimte.

Investeringskosten

De toename in verkeersvolume vereist geen aanvullende investering ten opzichte van de berekeningen voor het huidige verkeer.

Exploitatie- en beheerkosten

Zie hierboven.

3.5.2 Optie 2

In de volgende subparagrafen zijn de organisatorische en technische consequenties van de stijging van het telecom- en internetverkeer apart behandeld. Een indicatie van de financiële consequenties van deze toename is tevens gegeven.

[20] Geschatte opslagcapaciteit voor de toegang tot internet via internetcafés zoals hierboven berekend.
[21] Geraamde opslagruimte voor de toegang tot internet via internetcafés zoals hierboven gecalculeerd.

3.5.2.1 Telecomverkeer: vaste telefonie

De organisatorische en technische gevolgen van de stijging van het vaste telefonieverkeer tezamen met een schatting van de bijbehorende kosten zijn hieronder uiteengezet.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het telecomverkeer met 25% in ongeveer 0,5TB (2TB[22] x 25%) additionele opslagcapaciteit.

Voor de bewaartermijn van 24 maanden leidt de stijging van het telecomverkeer met 25% tot circa 1TB (4TB[23] x 25%) additionele opslagruimte.

Gezien de bij de overheidsinstantie ingerichte processen en de uitvoerige toelichting, zoals hierboven is aangegeven, kan worden verwacht dat er in vergelijking met haar huidige situatie sprake is van gelimiteerde organisatorische consequenties.

Technische consequenties

Rekeninghoudend met de bij de overheidsinstantie in gebruik zijnde infrastructuur kan worden gesteld dat er in vergelijking met haar huidige situatie sprake is van beperkte technische consequenties. De verwachting is dat voornamelijk additionele hardware nodig is die onder andere is geëquipeerd met de geëiste opslagcapaciteit, zoals hierboven berekend.

Investeringskosten

Voor de bewaartermijn van 12 maanden bedragen de investeringskosten naar verwachting circa EUR 300.340.

Voor de bewaartermijn van 24 maanden zullen de investeringskosten naar schatting uitkomen op ongeveer EUR 333.023.

De calculatie van deze kosten is gebaseerd op de hierboven uitgelegde berekeningen en gemaakte aannames. De investeringskosten voor de beide bewaartermijnen zijn in tabel 20 weergegeven.

[22] Geraamde overheidsopslag voor de vaste telefonie zoals hierboven gecalculeerd.
[23] Geschatte overheidsopslag voor de vaste telefonie zoals hierboven berekend.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	EUR 7.797	EUR 15.594
Hardware	EUR 29.810	EUR 53.896
Wijziging applicaties:		
- Opslag	Nihil	Nihil
- Bevraging	EUR 250.000	EUR 250.000
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	EUR 11.533	EUR 11.533
Uitwijk	Nihil	Nihil
Installatie	EUR 1.200	EUR 2.000
Totaal:	EUR 300.340	EUR 333.023

Tabel 20. Geraamde totale investeringskosten voor het vaste telefonieverkeer bij de verkeerstoename met 25%.

Exploitatie- en beheerkosten

Voor de bewaartermijn van 12 maanden bedragen de exploitatie- en beheerkosten naar verwachting circa EUR 422.000.

Voor de bewaartermijn van 24 maanden zullen de exploitatie- en beheerkosten naar schatting uitkomen op ongeveer EUR 489.000.

De berekening van deze kosten is gebaseerd op de hierboven uitgelegde calculaties en gemaakte aannames. De exploitatie- en beheerkosten voor de bewaartermijnen van 12 en 24 maanden zijn in tabel 21 gepresenteerd.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel:		
- Opslag	EUR 40.000	EUR 80.000
- Bevraging	EUR 50.000	EUR 50.000
Inhuur	Nihil	Nihil
Huisvesting	EUR 10.000	EUR 20.000
Huurlijnen:		
- Opslag	Nihil	EUR 17.000
- Bevraging	EUR 22.000	EUR 22.000
Vergoedingen	EUR 300.000	EUR 300.000
Totaal:	EUR 422.000	EUR 489.000

Tabel 21. Geschatte totale exploitatie- en beheerkosten voor het vaste telefonieverkeer bij de verkeersstijging met 25%.

3.5.2.2 Telecomverkeer: mobiele telefonie

De organisatorische en technische gevolgen van de toename van het mobiele telefonieverkeer tezamen met een raming van de gepaard gaande kosten zijn hieronder uitgelegd.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het telecomverkeer met 25% in ongeveer 1,5TB (6TB[24] x 25%) additionele opslagcapaciteit. In totaal wordt 7,5TB opgeslagen.

Voor de bewaartermijn van 24 maanden leidt de stijging van het telecomverkeer met 25% tot circa 3TB (12TB[25] x 25%) bijkomende opslagruimte. In totaal wordt 15TB opgeslagen.

De gevolgen voor de organisatorische procedures bij de overheidsinstantie zijn hierboven reeds aan de orde geweest.

Technische consequenties

De verwachting is dat hoofdzakelijk extra hardware noodzakelijk is ten behoeve van de hierboven gecalculeerde additionele overheidsopslag met de bijbehorende licenties.

Investeringskosten

Voor de bewaartermijn van 12 maanden bedragen de investeringskosten naar verwachting circa EUR 98.387.

Voor de bewaartermijn van 24 maanden zullen de investeringskosten naar schatting uitkomen op ongeveer EUR 182.374.

De calculatie van deze kosten is gebaseerd op de hierboven toegelichte berekeningen en gemaakte aannames. De investeringskosten voor de beide bewaartermijnen zijn in tabel 22 getoond.

[24] Geschatte overheidsopslag voor de mobiele telefonie zoals hierboven berekend.
[25] Geraamde overheidsopslag voor de mobiele telefonie zoals hierboven gecalculeerd.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Softwarelicenties	EUR 15.594	EUR 31.188
Hardware	EUR 69.260	EUR 124.120
Wijziging applicaties	Nihil	Nihil
Nieuwe applicaties	Nihil	Nihil
Upgrades	Nihil	Nihil
Back-upmedia	EUR 11.533	EUR 23.066
Uitwijk	Nihil	Nihil
Installatie	EUR 2.000	EUR 4.000
Totaal:	EUR 98.387	EUR 182.374

Tabel 22. Geraamde totale investeringskosten voor het mobiele telefonieverkeer bij de verkeerstoename met 25%.

Exploitatie- en beheerkosten

Voor de bewaartermijn van 12 maanden bedragen de exploitatie- en beheerkosten naar verwachting circa EUR 167.000.

Voor de bewaartermijn van 24 maanden zullen de exploitatie- en beheerkosten naar schatting op ongeveer EUR 367.000 uitkomen.

De berekening van deze kosten is gebaseerd op de hierboven beschreven calculatie en gemaakte aannames. Een overzicht van de exploitatie- en beheerkosten voor de beide bewaartermijnen is in figuur 23 gegeven.

	Bewaartermijn 12 maanden	**Bewaartermijn 24 maanden**
Personeel	EUR 120.000	EUR 280.000
Inhuur	Nihil	Nihil
Huisvesting	EUR 30.000	EUR 70.000
Huurlijnen	EUR 17.000	EUR 17.000
Vergoedingen	Nihil	Nihil
Totaal:	EUR 167.000	EUR 367.000

Tabel 23. Geschatte totale exploitatie- en beheerkosten voor het mobiele telefonieverkeer bij de verkeersstijging met 25%.

3.5.2.3 Internetverkeer: internettoegang

De organisatorische en technische gevolgen van de toename van het verkeer betreffende de internettoegang tezamen met een schatting van de bijbehorende kosten zijn hieronder uiteengezet.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het internetverkeer met 100% in ongeveer 1,5PB (730TB[26] x 2) additionele opslagcapaciteit.

Voor de bewaartermijn van 24 maanden leidt de stijging van het internetverkeer met 100% tot circa 3PB (1,5PB[27] x 2) bijkomende opslagruimte.

Investeringskosten

Voor de opslag van 1,5PB voor een periode van 12 maanden is een investering van EUR 10 miljoen vereist. Voor de opslag van 3PB voor een periode van 24 maanden is dit EUR 17 miljoen.

Exploitatie- en beheerkosten

Deze kosten zijn respectievelijk EUR 1,5 miljoen en EUR 2,2 miljoen voor de periode van 12 en 24 maanden.

3.5.2.4 Internetverkeer: e-mail

De organisatorische en technische gevolgen van de toename van het verkeer met betrekking tot de e-maildienst tezamen met een raming van de geassocieerde kosten zijn hieronder besproken.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het internetverkeer met 100% in ongeveer 55TB (26TB[28] x 2) additionele opslagcapaciteit.

Voor de bewaartermijn van 24 maanden leidt de stijging van het internetverkeer met 100% tot circa 105TB (52TB[29] x 2) bijkomende opslagruimte.

Investeringskosten

Een leverancier gaf een indicatie van EUR 520.000 aan investeringskosten voor de opslag van 55TB voor 12 maanden en EUR 1 miljoen voor 105TB voor 24 maanden.

[26] Geraamde overheidsopslag voor de internettoegang zoals hierboven gecalculeerd.
[27] Geschatte overheidsopslag voor de internettoegang zoals hierboven berekend.
[28] Geschatte overheidsopslag voor de e-mail zoals hierboven berekend.
[29] Geraamde overheidsopslag voor de e-mail zoals hierboven gecalculeerd

Exploitatie- en beheerkosten

Een aantal kosten is afhankelijk van de wensen van de behoeftestellers en keuzes voor de implementatie. Een schatting is EUR 150.000 voor de periode van 12 maanden en EUR 220.000 voor 24 maanden.

3.5.2.5 Internetverkeer: internetcafé

De organisatorische en technische gevolgen van de toename van het verkeer aangaande de toegang tot internet via internetcafés tezamen met een schatting van de gerelateerde kosten zijn hieronder beschreven.

Organisatorische consequenties

Voor de bewaartermijn van 12 maanden resulteert de toename van het internetverkeer met 100% in ongeveer 5,5TB (2,7TB[30] x 2) additionele opslagcapaciteit. Hierbij is met enige overhead rekening gehouden.

Voor de bewaartermijn van 24 maanden leidt de stijging van het internetverkeer met 100% tot circa 11TB (5,5TB[31] x 2) bijkomende opslagruimte.

Investeringskosten

De investeringskosten voor de bewaartermijnen van 12 en 24 maanden voor 5,5TB en 11TB wordt respectievelijk geschat op EUR 93.085 en EUR 154.347.

Exploitatie- en beheerkosten

De exploitatie- en beheerkosten voor de bewaartermijnen van 12 en 24 maanden voor 5,5TB en 11TB wordt respectievelijk geschat op EUR 167.000 en EUR 317.000.

3.5.3 Totaal kostenoverzicht

Het totale overzicht van de geraamde kosten van optie 1 en optie 2 is respectievelijk in de tabel 24 en tabel 25 getoond. Hierbij is rekening gehouden met de uitgangspunten betreffende de bewaartermijn van 12 maanden en de bewaartermijn van 24 maanden. De totstandkoming van deze kosten is hierboven separaat toegelicht.

[30] Geschatte overheidsopslag voor de toegang tot internet via internetcafés zoals hierboven berekend.
[31] Geraamde overheidsopslag voor de toegang tot internet via internetcafés zoals hierboven gecalculeerd.

Optie 1 voor gekozen aanbieder	**Markt-aandeel**	**Bewaartermijn 12 maanden**	**Bewaartermijn 24 maanden**
Initiële investeringskosten:			
Telecomverkeer: vaste telefonie	70%	EUR 19.794	EUR 31.024
Telecomverkeer: mobiele telefonie	30-40%	EUR 25.524	EUR 48.618
Internetverkeer: internettoegang	10%	EUR 2,2 - EUR 3	EUR 3 - EUR 4
Internetverkeer: e-mail	10%	miljoen	miljoen
Internetverkeer: internetcafé	1%	EUR 48.618	EUR 97.236
		EUR 2.730	EUR 2.730
Jaarlijkse exploitatie- en beheerkosten:			
Telecomverkeer: vaste telefonie	70%	EUR 40.000	EUR 40.000
Telecomverkeer: mobiele telefonie	30-40%	EUR 80.000	EUR 80.000
Internetverkeer: internettoegang	10%		
- Personeel bevraging		EUR 20.000	EUR 20.000
Internetverkeer: e-mail	10%		
- Personeel bevraging		EUR 20.000	EUR 20.000
Internetverkeer: internetcafé	1%	EUR 8.000	EUR 8.000

Tabel 24. Overzicht geraamde kosten van de consequenties van de toename van het telecommunicatieverkeer voor optie 1.

Optie 2 gesommeerd voor overheid	**Bewaartermijn 12 maanden**	**Bewaartermijn 24 maanden**
Initiële investeringskosten:		
Telecomverkeer: vaste telefonie	EUR 300.340	EUR 333.023
Telecomverkeer: mobiele telefonie	EUR 98.387	EUR 182.374
Internetverkeer: internettoegang	EUR 10 miljoen	EUR 17 miljoen
Internetverkeer: e-mail	EUR 520.000	EUR 1 miljoen
Internetverkeer: internetcafé	EUR 93.085	EUR 154.347
Jaarlijkse exploitatie- en beheerkosten:		
Telecomverkeer: vaste telefonie	EUR 422.000	EUR 489.000
Telecomverkeer: mobiele telefonie	EUR 167.000	EUR 367.000
Internetverkeer: internettoegang	EUR 1,5 miljoen	EUR 2,2 miljoen
Internetverkeer: e-mail	EUR 150.000	EUR 200.000
Internetverkeer: internetcafé	EUR 167.000	EUR 317.000

Tabel 25. Overzicht geschatte kosten van de consequenties van de toename van het telecommunicatieverkeer voor optie 2.

4 Beveiligingsaspecten

De beveiligingsaspecten voor de telecommunicatieaanbieders (optie 1) en voor de overheid (optie 2) zijn hieronder beschreven. Aangezien de historische verkeersgegevens[32] zoals gepositioneerd in het ontwerp 'Besluit vorderen gegevens telecommunicatie' onder andere persoonsgegevens bevatten, dienen deze in overeenstemming met de WBP te worden beveiligd.

4.1 Begrippen

In het kader van de WBP kent de beveiliging van de persoonsgegevens een drietal kwaliteitsaspecten, te weten: exclusiviteit, integriteit en continuïteit. De definities van deze aspecten zijn hieronder gegeven:[33]

- Exclusiviteit. Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik \maken van persoonsgegevens.

- Integriteit. De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.

- Continuïteit. De persoonsgegevens en de daarvan afgeleide informatie moet zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Continuïteit wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.

Aangezien diverse soorten persoonsgegevens in verschillende sectoren en markten worden verwerkt, kent de WBP een aantal risicoklassen. De vereiste beveiligingsmaatregelen verschillen per risicoklasse. Uitgegaan is van 4 zogeheten 'risicoklassen' waarvan de opbouw cumulatief is. Dit wil zeggen dat hogere klassen bijkomende normen aangeven die bij deze klasse passen. De risicoklassen zijn hieronder nader uiteengezet:[34]

- Risicoklasse 0, ook aangeduid als public niveau, representeert de openbare persoonsgegevens. Bij deze klasse gaat het om de persoonsgegevens waarvan algemeen is aanvaard dat deze, bij het gewenste gebruik, geen risico's tot gevolg hebben voor de betrokkene. Als voorbeelden hiervan kunnen de telefoonboeken en publieke internetsites worden genoemd.

- Risicoklasse I, ook basis niveau genoemd, symboliseert de situatie waarin de risico's voor de betrokkene bij verlies, onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zodanig zijn dat standaard informatiebeveiligingsmaatregelen toereikend zijn. Hierbij gaat het

[32] In het ontwerp 'Besluit vorderen gegevens telecommunicatie' wordt de term verkeersgegevens omschreven als gegevens over de gebruiker en het telecommunicatieverkeer betreffende deze gebruiker.
[33] Bron: Blarkom, G.W. van, en J.J. Borking, Beveiliging van persoonsgegevens: Achtergrondstudies en Verkenningen 23, Registratiekamer, Den Haag, april 2001.
[34] Bron: Blarkom, G.W. van, en J.J. Borking, Beveiliging van persoonsgegevens: Achtergrondstudies en Verkenningen 23, Registratiekamer, Den Haag, april 2001.

om een beperkt aantal persoonsgegevens dat onder andere lidmaatschappen en arbeidsrelaties betreffen.

- Risicoklasse II, ook aangeduid als verhoogd risico, geeft aan dat extra negatieve gevolgen bestaan voor de betrokkene bij verlies, onbevoegd of onzorgvuldig gebruik van de persoonsgegevens. De hiervoor te nemen informatiebeveiligingsmaatregelen dienen te voldoen aan hogere normen dan die voor het basis niveau. In risicoklasse II vallen onder andere de gegevens die de door de handelinformatiebureaus worden verwerkt voor de kredietinformatie of voor de schuldsanering, en de gegevens die de gehele of grote delen van de bevolking betreffen.

- Risicoklasse III, ook hoog risico genoemd, representeert de situatie waarin de uitkomst van de verwerking van meerdere verzamelingen van bijzondere persoonsgegevens een dermate vergroot risico voor de betrokkene met zich meebrengt dat het is gerechtvaardigd deze verwerking in de risicoklasse III te positioneren. De hiervoor te nemen informatiebeveiligingsmaatregelen dienen te voldoen aan de hoogste normen. In deze risicoklasse vallen de verwerkingen van persoonsgegevens die betrekking hebben op de diensten met bijzondere bevoegdheden en verwerkingen, waarbij de belangen van de betrokkene ernstig kunnen worden geschaad in geval dit onzorgvuldig of onbevoegd plaatsvindt.

4.2 Optie 1

Door de behoeftestellers worden verzoeken ingediend bij de aanbieders om kennis te nemen van de verkeersgegevens. Deze verzoeken dienen met de nodige zorgvuldigheid door de aanbieders te worden behandeld. De behoeftestellers zijn in 2 groepen te onderkennen, waarbij de rubricering van de verzoeken verschillen. Wanneer behoeftestellers een aanbieder op basis van de Wet op de Inlichtingen- en Veiligheidsdiensten benaderen met een verzoek om kennisname van verkeersgegevens, is dit verzoek tenminste als Stg. CONFIDENTIEEL gerubriceerd. Dit impliceert dat deze verzoeken conform het gestelde in het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie moeten worden behandeld.

Wanneer behoeftestellers een aanbieder in het kader van de opsporingstaak benaderen met een verzoek om kennisname van verkeersgegevens, is dit verzoek vertrouwelijk van aard maar conform het gestelde in het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie ongerubriceerd.

4.2.1 Telecommunicatiewet

Het artikel 13.5 van de Telecommunicatiewet geeft het volgende aan. Het eerste lid eist dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten verplicht zijn gegevens aangaande een bijzondere last dan wel een toestemming op grond van de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 als bedoeld in artikel 13.2 en informatieverstrekkingen als bedoeld in artikel 13.4 te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten betreffende deze gegevens. Het tweede lid beschrijft dat

bij algemene maatregel van bestuur regels kunnen worden gesteld met betrekking tot de te nemen maatregelen in verband met de beveiliging, bedoeld in het eerste lid.

4.2.2 Besluit beveiliging gegevens aftappen telecommunicatie

Er ligt een besluit van 28 oktober 2003, houdende regels aangaande de door de aanbieders te treffen beveiligingsmaatregelen ten aanzien van gegevens met betrekking tot het aftappen en opnemen van telecommunicatie. Dit wordt 'Besluit beveiliging gegevens aftappen telecommunicatie' genoemd en is nog niet van kracht. Het besluit betreft de verplichting voor de telecommunicatieaanbieders om te zorgen voor een adequate beveiliging van de gegevens en informatie. Het vertaalt feitelijk de in het eerste lid van het artikel 13.5 abstract geformuleerde zorgplicht naar een aantal door de aanbieder te nemen acties. Het besluit kent de onderstaande kernelementen:[35]

- Een explicitering van de aspecten waarop de te implementeren beveiligingsmaatregelen dienen te focussen. Deze moeten bestaan uit de maatregelen gericht op:
  - De personen die voor de aanbieder werken.
  - De toegang tot de gebouwen en ruimten waarin de gegevens en informatie aanwezig zijn.
  - Een deugdelijke werking en beveiliging van het informatiesysteem waarin de gegevens en informatie worden verwerkt.
  - Het voorkomen, vaststellen en onderzoeken van een ongeautoriseerde inbreuk op de vertrouwelijkheid van de gegevens en informatie.
  - De gevallen van calamiteiten.
- Een overzicht van de maatregelen die verplicht dienen te worden getroffen, te weten:
  - Beveiligingseisen ten aanzien van een functionaris die is belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen.
  - Beveiligingseisen ten aanzien van personeel, waarbij onder andere wordt gedacht aan functiebeschrijving en geheimhoudingsverklaring.
  - Fysieke beveiliging en beveiliging van de omgeving. Voorbeelden hiervan zijn de detectie van de ongeautoriseerde toegang en pogingen tot de fysieke ruimte en het achteraf kunnen controleren en herleiden van het binnentreden en het verlaten van de ruimte op individueel niveau.

[35] Bron: Staatsblad van het Koninkrijk der Nederlanden, Besluit beveiliging gegevens aftappen telecommunicatie, jaargang 2003.

- Beheer van communicatie- en bedieningsprocessen. Onder meer wordt gedacht aan de rubricering van de informatie en aan de verwijdering en vernietiging van de informatie en gegevens op een onomkeerbare manier.

- Toegangsbeveiliging van geautomatiseerde informatiesystemen. Als voorbeelden hiervan kunnen de beperking van het aantal foutieve inlogpogingen (tot 3 keer) en het persoonsgebonden vastleggen van de handelingen betreffende de verwerking van de informatie en de gegevens worden genoemd.

- Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen, waarbij onder andere wordt gedacht aan het controleerbaar zijn van de wijzigingen in de apparatuur, software of procedures die de beveiliging van de informatie en de gegevens beïnvloeden, en de reparatie aan informatiesystemen waarin de informatie en gegevens worden verwerkt op locatie.

- De eis dat de te implementeren maatregelen in een beveiligingsplan worden opgenomen.

- De plicht dat de aanbieder uitsluitend personeel inzet die op basis van de Wet op de veiligheidsonderzoeken beschikken over een verklaring van geen bezwaar voor de uitvoering van de taplasten of verzoeken om informatie. De aanbieder zorgt tevens dat het bij de processgang betrokken personeel de geëiste geheimhouding volgt.

- De te treffen maatregelen bij ongeautoriseerde inbreuken op de vertrouwelijkheid.

- Maatregelen voor het geval dat een aanbieder werkzaamheden uitbesteed aan een derde partij.

Het besluit houdt rekening met het toezicht op de naleving van de beveiligingsplicht van de aanbieder. Deze taak is vanaf 1 september 2002 belegd bij het Agentschap Telecom van het Ministerie van Economische Zaken. Het besluit reikt tevens argumenten (zoals lage en moeilijk in te schatten kosten) aan op basis waarvan wordt gesteld dat de met de uitvoering gepaard gaande kosten als beperkt kunnen worden beschouwd. Het besluit is voor advies aan het Adviescollege Toetsing Administratieve Lasten (ACTAL) voorgelegd. Dit college heeft medegedeeld dat het besluit niet wordt geselecteerd voor een ACTAL-toets op de consequenties hiervan voor de administratieve lasten voor de aanbieders. De argumentatie hiervoor is dat de omvang van de door het besluit bezorgde administratieve lasten is gelimiteerd. Wel is in het besluit aangegeven dat kosten welke zijn verbonden aan de uitvoering van veiligheidsonderzoeken op grond van de Wet veiligheidsonderzoeken, door de staat worden betaald.

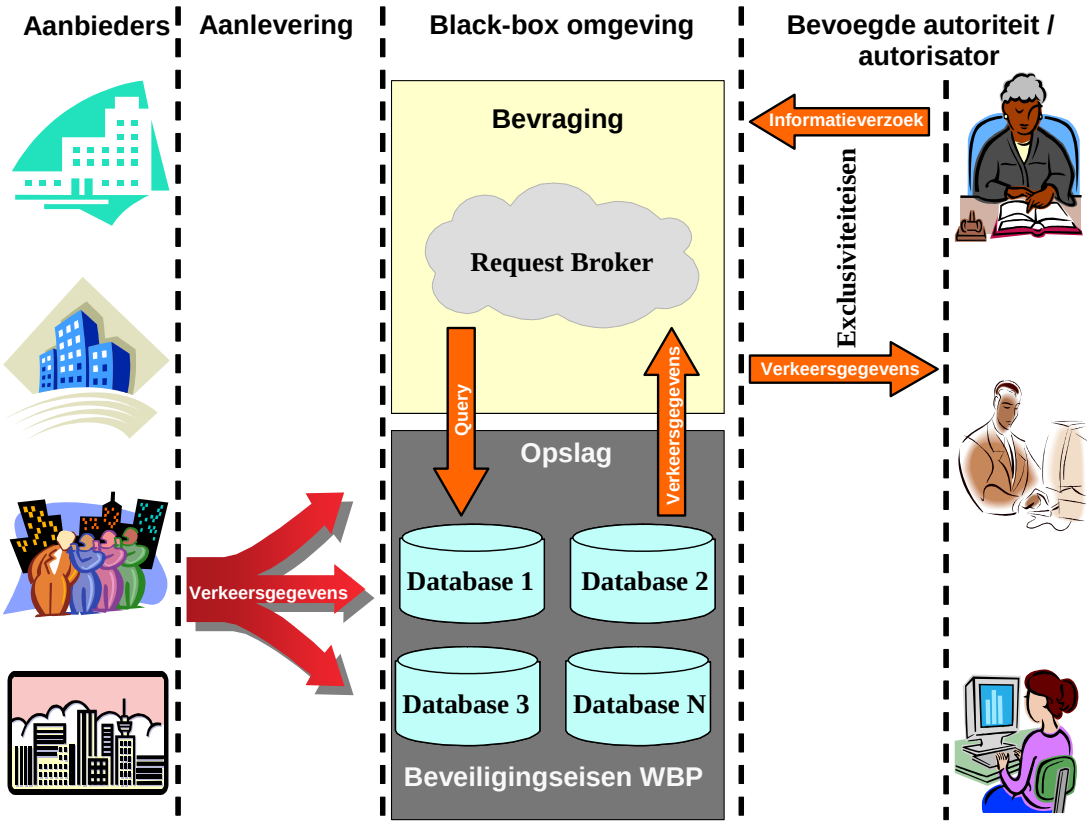
4.2.3 Algemene opmerkingen

Met het ‘Besluit beveiliging gegevens aftappen telecommunicatie’ wordt de in het artikel 13.5 van de Telecommunicatiewet geformuleerde zorgplicht vertaald naar een aantal door de aanbieders te nemen acties. De explicitering en de implementatie van de maatregelen alsmede het opnemen hiervan in een beveiligingsplan vormen feitelijk de essentie van het besluit. Uit de prak-

tijk blijkt dat de telefonieaanbieders (en sommige grote ISPs) in het bijzonder aandacht hebben voor beveiliging. Zij beschikken meestal over een beveiligingsplan, waarvoor de Code voor Informatiebeveiliging hoofdzakelijk als leidraad wordt gehanteerd. Deze aanbieders zijn zich goed bewust van de imago of financiële schade die beveiligingsincidenten tot gevolg kunnen hebben en spelen daarop optimaal in. Een verantwoordelijke beveiligingsfunctionaris is daarbij vaak ook niet weg te denken. Verondersteld wordt dat de telefonieaanbieders reeds de benodigde beveiligingsmaatregelen hebben getroffen gezien de ervaring die zij met de behoeftestellers hebben en rekeninghoudend met de gevallen waarbij de veiligheid van de staat in het geding is. Met het onderhavige besluit wordt geconcreteriseerd aan welke beveiligingseisen de (resterende) aanbieders dienen te voldoen.

4.2.4 Recapitulatie

Het ‘Besluit beveiliging gegevens aftappen telecommunicatie’ heeft mede betrekking op de inhoud van de communicatie. Aangenomen kan worden dat voor dit gegevenstype in feite de zwaarste beveiligingseisen (risicoklasse III) geldt, aangezien het zowel de gebruikersgegevens als de verkeersgegevens betreft. Indien een gesprek wordt afgetapt, zijn de betrokken individuen (gegevens met betrekking tot de gebruikers van de dienst) alsmede hun telefoonnummers (gegevens aangaande de netwerken en diensten) reeds bekend. Voor de opslag van de historische verkeersgegevens betekent dit concreet dat aan de beveiligingseisen van de WBP dient te worden voldaan. Wanneer deze opgeslagen verkeersgegevens worden bevraagd, dient te worden gezorgd dat de exclusiviteit van de opgevraagde gegevens wordt gewaarborgd, zodat het welslagen van een strafrechtelijk onderzoek of de veiligheid van de staat niet in het geding komt. Het bovenstaande is in figuur 3 schematisch weergegeven waarbij is uitgegaan van het blackboxconcept.



Figuur 3. Beveiligingseisen bij opslag en bevraging.

Uitgaande van de in het besluit voorgeschreven beveiligingsmaatregelen kan worden gesteld dat in voldoende mate rekening wordt gehouden met de 3 kwaliteitsaspecten van WBP betreffende de opslag- en bevragingsbeveiliging van persoonsgegevens. Het besluit speelt eveneens in op de gepaard gaande financiële aspecten en op de gevallen waarbij sprake kan zijn van uitbesteding van activiteiten aan derde partijen. Met het onderhavige besluit wordt een redelijke mate van zekerheid verkregen omtrent de beveiliging bij de aanbieders.

4.3 Optie 2

De behoeftestellers bevragen de in de black-boxen opgeslagen gegevens door middel van een applicatie. De overheidsinstantie treedt op als de beheerder van deze gegevens die in feite eigendom van de aanbieders zijn. De bevraging van de in de black-boxen residente gegevens wordt als Stg. CONFIDENTIEEL gerubriceerd, aangezien deze tevens informatie ten behoeve van de Inlichtingen- en Veiligheidsdiensten bevat.

4.3.1 Voorschrift Informatiebeveiliging Rijksdienst (VIR)

Het VIR behelst algemene regels voor de informatiebeveiliging bij de rijksoverheid. Dit voorschrift stelt geen concrete beveiligingseisen en biedt in feite een methodiek teneinde door middel van een afhankelijkheidsanalyse de eisen ten aanzien van betrouwbaarheid te bepalen. Met dit kwaliteitsaspect wordt de mate bedoeld waarin de organisatie zich kan verlaten op een informatiesysteem ten behoeve van haar informatievoorziening. De betrouwbaarheidseisen worden in het VIR onderverdeeld in exclusiviteit, integriteit en beschikbaarheid (oftewel continuïteit).

4.3.2 Basisvoorzieningen Informatiebeveiliging Ministerie van Justitie

Het Ministerie van Justitie heeft basisvoorzieningen beschreven die voor de beveiliging van de informatievoorziening worden gehanteerd. Deze maatregelen zijn afgeleid van het voor het ministerie opgestelde informatiebeveiligingsbeleid, hetgeen een justitie specifieke invulling is van het VIR. Bij het ontwikkelen van dit beleid is mede rekening gehouden met de wet- en regelgeving, de Code voor Informatiebeveiliging, het onderling zijn verbonden van alle onderdelen van JustitieNet en PolitieNet, en het vooral gebruikmaken van persoonsgebonden gegevens. Het beveiligingsbeleid is de basis voor het vaststellen en het implementeren van de maatregelen en is door de Secretaris Generaal (SG) goedgekeurd. Deze stelt het beleid ieder 2 jaar opnieuw vast, waarvoor het advies van de Directie Informatisering in samenspraak met de informatiebeveiligingsambtenaar (IBVA) wordt gebruikt. Hoofdpunten van dit beleid zijn:[36]

- Het informatiebeveiligingsbeleid is van toepassing op het gehele Justitie-concern, zowel het centrale bestuursdepartement als de afzonderlijke hoofdkantoren en diensten en daaronder ressorterende organisatie-eenheden, inclusief de intern verzelfstandigde onderdelen, zoals agentschappen en zelfstandige bestuursorganen.

- Informatiebeveiliging vormt een onderdeel van de kwaliteitszorg voor bedrijfsprocessen en ondersteunende informatiesystemen en is gericht op het kwaliteitsaspect betrouwbaarheid. Hieronder worden exclusiviteit, integriteit en beschikbaarheid (continuïteit) verstaan.

- Het integrale management is primair verantwoordelijk voor het op concernniveau vastgestelde informatiebeveiligingsbeleid.

4.3.3 Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI)

Een aanvulling op het VIR is VIR-BI dat op de bescherming van exclusiviteit van de bijzondere informatie bij de rijksdienst is gericht. Met deze term worden staatsgeheimen en overige bijzondere informatie bedoeld, waarvan kennisname door niet bevoegden nadelige gevolgen kan hebben voor de belangen van de staat, van zijn bondgenoten of van één of meer ministeries. Voor de integriteit en beschikbaarheid van de bijzondere informatie wordt volstaan met de afhankelijkheids- en kwetsbaarheidsanalyse conform het VIR.

[36] Bron: Directie Informatisering, Basisvoorzieningen Informatiebeveiliging Ministerie van Justitie, versie 1.0 definitief, 8 maart 2000.

4.3.4 Informatiebeveiliging bij de overheidsinstantie

De hierboven genoemde instantie maakt onderdeel uit van de overheid en houdt zich derhalve aan het opgestelde informatiebeveiligingbeleid van het ministerie waaronder zij valt. De overheidsinstantie heeft een informatiebeveiligingsplan ontwikkeld, hetgeen door middel van self-assessments tot stand is gekomen. De daarin opgenomen maatregelen vloeien voort uit het voor het ministerie opgestelde informatiebeveiligingbeleid. Voor de realisatie van dit beleid hanteert de overheidsinstantie op bedrijfsniveau de onderstaande beleidsuitgangspunten:

- De beheerfunctie van het informatiesysteem van de klanten wordt ongehinderd en zonder aantasting van de integriteit vervuld.

- Met de implementatie van de noodzakelijke maatregelen wordt gezorgd dat de continuïteit van het informatiesysteem (indien verantwoordelijkheid van de overheidsinstantie) van de klanten en de gerelateerde dienstverlening wordt gewaarborgd.

- Zorg wordt gedragen voor de beschikbaarheid, integriteit en exclusiviteit van de beschikbaargestelde of toevertrouwde informatie waartoe de overheidsinstantie krachtens de beheerfunctie toegang heeft.

Ten behoeve van de uitvoering houdt de overheidsinstantie zich aan de door het ministerie opgestelde voorschriften door:

- basisvoorzieningen Informatiebeveiliging Ministerie van Justitie en VIR-BI in te voeren;

- periodieke Afhankelijkheids- en Kwetsbaarheidanalyse (A&K-analyse) uit te voeren en de hieruit resulterende maatregelen in te voeren;

- medewerkers kennis te laten nemen van de justitie brede beveiligingsvoorschriften;

- een informatiebeveiligingsplan te implementeren en te onderhouden;

- een beveiligingsfunctionaris te benoemen voor de dagelijkse coördinatie van de beveiligingszaken;

- toestemming te vragen bij de directie indien wordt afgeweken van procedures en richtlijnen die op beveiliging betrekking hebben.

De overheidsinstantie heeft de stand van zaken omtrent de invoering van het informatiebeveiligingsbeleid en het VIR-BI onderzocht. Uit dit onderzoek is gebleken dat een groot gedeelte van de te treffen maatregelen uit deze beveiligingsvoorschriften zijn geïmplementeerd. Een inventarisatie van de resterende te nemen maatregelen is opgesteld, waarop acties zijn gedefinieerd. Voor de uitvoering van de risicoanalyse (CRAMM) werd een apart project gedefinieerd dat inmiddels is afgerond.

De overheidsinstantie is voornemens een procesmanager aan te stellen die eveneens de rol van de informatiebeveiligingsfunctionaris zal vervullen. Op beveiligingsgebied streeft deze instantie ernaar de beveiliging zodanig in te richten dat de certificering mogelijk is.

Doelstellingen ten behoeve van het toezicht op de beveiliging bij de overheidsinstantie zijn geformuleerd. Hiervoor wordt door de behoeftestellers alsmede door de aanbieders input geleverd. De werking van de getroffen maatregelen wordt door middel van een technische penetratietest onderzocht. De hieruit voortkomende maatregelen dienen te worden geïmplementeerd.

De met de beveiliging gepaard gaande kosten dienen in het budget van de overheidsinstantie te worden opgenomen.

4.3.5 Recapitulatie

Op grond van het bovenstaande kan worden gesteld dat de beveiliging bij de overheidsinstantie op adequate wijze in de bestaande structuur kan worden ingebed. Naast het feit dat aansluiting is gezocht met het informatiebeveiligingsbeleid van het ministerie waaronder deze instantie valt, wordt ook aandacht geschonken aan de geldende voorschriften. Er moet worden voldaan aan de door de WBP-gestelde beveiligingseisen voor de opslag van de historische verkeersgegevens. Aangezien VIR-BI deze wet overstijgt, wordt gesteld dat eveneens wordt voldaan aan de specifieke exclusiviteitseisen die aan de bevraging worden gesteld indien de overheidsinstantie volledig aan VIR-BI voldoet.

Aangezien de hierboven genoemde instantie een onderdeel van de overheid is, kan een beter inzicht worden verschaft in de werking van de geïmplementeerde beveiligingsmaatregelen. Hierdoor wordt de stand van zaken rondom de beveiliging zichtbaarder. Als gevolg hiervan wordt de kans verhoogd dat dit aspect als transparant wordt ervaren.

5 Wet- en regelgeving

5.1 Scope

Er is uitdrukkelijk niet ingegaan op de juridische aspecten van een bewaarverplichting op zichzelf (de legitimiteit, proportionaliteit, effectiviteit, wettelijke verankering, doelstelling, en dergelijke). Ook werd geabstraheerd van de doeleinden waarvoor bevraging van de bewaarde historische gegevens is toegestaan, of zou moeten zijn. Alhoewel er op deze gebieden veel discussie wordt gevoerd en er op het juridische vlak veel verschillende standpunten worden ingenomen (bijvoorbeeld ten aanzien van de wettelijke bevoegdheden op grond waarvan gegevens gevorderd mogen worden, het noodzakelijkheidsvereiste van artikel 8 EVRM, het gebruik van de gegevens doelen zoals preventie, verkennend onderzoek, en dergelijke, het opvragen van gegevens van niet-verdachte personen, het gebruik van de gegevens voor datamining en profielontwikkeling, enzovoort), is ervoor gekozen deze aspecten buiten beschouwing te laten.

5.2 Optie 1

Optie 1 is in deze fase niet nader besproken.

5.3 Optie 2

Ten aanzien van deze optie kunnen 2 subvarianten worden onderscheiden, te weten: optie 2a en optie 2b. Hierbij zit het essentiële verschil in de verantwoordelijkheid die wordt gedragen ten aanzien van de bewaarde gegevens en het daadwerkelijke moment van verstrekking van de gegevens (in de zin van het buiten de macht van de aanbieders brengen van de betreffende gegevens) aan een derde. Deze 2 opties worden hieronder nader besproken.

5.3.1 Optie 2a

Bij optie 2a kan in de visie van de opdrachtgever worden gedacht aan de opzet van een systeem van gedecentraliseerde databases die kunnen worden bevraagd door een centraal zoeksysteem dat wordt beheerd door de overheid. De in de databases opgeslagen gegevens zijn en blijven de verantwoordelijkheid van de aanbieders die de gegevens aanleveren. Voor deze variant staat de huidige overheidsinstantie[37] en het bij deze instantie in gebruik zijnde model. Hierbij blijft de informatie ‘eigendom van’ de telecommunicatieaanbieders, doch wordt deze door middel van ‘black boxes’ ter bevraging beschikbaar gehouden door het geautomatiseerde bevragingssys-

[37] Zie hieromtrent het Besluit van 26 januari 2000, houdende regels voor de verstrekking van gegevens door aanbieders van openbare telecommunicatienetwerken en –diensten met het oog op het onderzoek van telecommunicatie (Besluit verstrekking gegevens telecommunicatie), Staatsblad 2000, 71, in werking per 1 september 2004.

teem, dat wordt beheerd door de overheidsinstantie. De telecommunicatieaanbieders blijven 'verantwoordelijke' in de zin van de WBP ten aanzien van de gegevens, de overheidsinstantie heeft te gelden als 'bewerker'. Een mogelijke vergelijking zou hier kunnen worden getrokken met een overslagbedrijf, dat goederen in bewaring neemt voor de eigenaar en deze eventueel aan bepaalde vastgestelde afnemers afgeeft. In de situatie van de opslag van verkeersgegevens is door de telecommunicatieaanbieders de bewaring uitbesteed aan de overheidsinstantie, dat rechtmatige bevragers toegang tot bepaalde gegevens mag (moet) verlenen. Van een daadwerkelijke verstrekking van gegevens door de telecommunicatieaanbieder is pas sprake op het moment van bevraging zelf, vóór die gebeurtenis heeft een onderdeel van de overheid geen (rechtmatige) toegang tot de gegevens. De informatie is echter wel al zodanig 'klaargezet' dat de bevrager er in voorkomende gevallen onverwijld over kan beschikken, op een efficiënte wijze. De overheidsinstantie handelt hierbij als een soort *information request broker*, een tussenschakel tussen bevragers (de behoeftestellers) en bewaarders (de telecommunicatieaanbieders). De overheidsinstantie fungeert tevens als centraal registratiepunt voor bevragingen. Hierdoor kan achteraf verantwoording worden afgelegd over de omvang en de (rechtmatigheid van de) doeleinden van de bevragingen. De overheidsinstantie ressorteert onder het Ministerie van Justitie.

5.3.2 Optie 2b

Optie 2b betreft de situatie dat de daadwerkelijke bewaring van gegevens rechtstreeks bij en onder de verantwoordelijkheid van een centraal overheidsorgaan plaatsvindt. Dit betreffende onderdeel heeft te gelden als de 'verantwoordelijke' in de zin van de WBP. In deze variant zouden telecommunicatieaanbieders de gegevens (bestanden) niet pas bij bevraging door de behoeftestellers aan deze derden verstrekken, maar is reeds eerder sprake van derdenverstrekking, namelijk op het moment van overdracht van de gegevens (bestanden) ter bewaring aan het betreffende onderdeel van de overheid. In dat geval zou niet zozeer een bewaarplicht behoeven te worden ingevoerd voor de telecommunicatieaanbieders, maar dient de verstrekking door telecommunicatieaanbieders ter bewaring en de subsequente bewaring door de overheid zelf te zijn/worden verankerd in de wet.

NB Uiteraard zullen ook in deze situatie 2b door de betreffende overheidsinstantie de wettelijke eisen die worden gesteld aan bevraging dienen te worden nageleefd, en zijn de gegevens niet beschikbaar voor ongelimiteerd gebruik.

5.4 Optie 3

Optie 3 zou nog kunnen zijn, dat de gegevens (en/of het bevragingssysteem) worden beheerd door een volledig van de overheid onafhankelijke organisatie, een derde partij naar het model van een Trusted Third Party (TTP). De bewaarplicht dient dan te zijn verankerd in de wet ten behoeve van de TTP. Ook hierbij vindt het voor het onderhavige onderzoek relevante verstrekkingsmoment reeds plaats bij overdracht van de te bewaren gegevens door de telecommunicatieaanbieder aan de TTP, niet pas bij bevraging.

5.5 Relevante wetgeving

5.5.1 WBP

Nu de te bewaren verkeersgegevens (tevens) persoonsgegevens betreffen, dient te worden uitgegaan van de regeling omtrent het verwerken van persoonsgegevens als vastgelegd in de WBP. Onder 'verwerking van persoonsgegevens' verstaat deze wet: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen en uitwissen of vernietigen van gegevens (artikel 1 onder b WBP). Een 'persoonsgegeven' is volgens de WBP 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon' (artikel 1 onder WBP).

Volgens artikel 2 WBP is de wet niet van toepassing op de verwerking van persoonsgegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de Inlichtingen- en Veiligheidsdiensten, alsmede door of ten behoeve van de uitvoering van de politietaak, omschreven in artikel 2 van de Politiewet 1993. Naar onze mening impliceert het instellen van een bewaarplicht met als doel het kunnen faciliteren van bevragingen door de politie, justitie en/of inlichtingen- en veiligheidsdiensten, zoals voorzien in het ontwerp-Kaderbesluit nog niet rechtstreeks dat de betreffende verwerking (de bewaring) ten behoeve van bevragers gebeurt, doch slechts dat de *mogelijkheid* hiertoe wordt geschapen. De gegevensbestanden blijven formeel in de macht van de telecommunicatieaanbieder, en blijven vallen onder diens verantwoordelijkheid. Het betreft hier voorts gegevens die (blijkens het Stratix-rapport) toch reeds bij de telecommunicatieaanbieder aanwezig zijn, en 'enkel' langer dienen te worden bewaard en onverwijld en op efficiënte wijze beschikbaar dienen te kunnen worden gemaakt. De WBP is derhalve naar onze mening onverkort van toepassing.

NB Het is de vraag of een zelfde conclusie kan worden getrokken ten aanzien van de situaties bij optie 2b en optie 3, waarbij de daadwerkelijke bewaring van gegevens niet gebeurt door de telecommunicatieaanbieders, maar door respectievelijk de overheid dan wel een TTP. In die situatie zal al de te bewaren informatie immers rechtstreeks en volledig worden verstrekt door telecommunicatieaanbieders aan de derde-bewaarder, met als uitsluitend doel de bewaring voor doeleinden als omschreven in het ontwerp-Kaderbesluit (gebruik ter preventie, onderzoek, detectie en vervolging van strafbare feiten, inclusief terrorisme).[38] Mogelijk dat in dat geval toepassing van artikel 2 WBP impliceert, dat de WBP niet van toepassing is op de verstrekking door de telecommunicatieaanbieders, doch de relevante (privacy)wetgeving in verband met de politie- en justitie en inlichtingen- en veiligheidsdiensten[39]. Voor het onderhavige onderzoek is

[38] Het feit dat preventie en (verkennend) onderzoek hierbij mede onder de bewaarplicht (en verstrekkingsreden) worden gebracht, kan problematisch zijn voor de Nederlandse juridische situatie. Op de rechtmatigheidsgrond voor bewaring en bevraging wordt in dit onderzoek echter niet nader ingegaan.

[39] De vraag is of de bewaring door de overheid c.q. een TTP in de voorziene omvang en voor alle in het ontwerp-Kaderbesluit bedoelde doeleinden als zodanig kan worden gelegitimeerd door bijvoorbeeld de Wet Politieregisters (art. 4); de legitimiteit van een bewaarplicht als zodanig is echter geen onderwerp van het onderhavige onderzoek. In geval van toepasselijkheid van bijvoorbeeld de Wet Politieregisters zal deze afweging echter wel dienen te worden gemaakt. Bewaring van informatie in de omvang en voor de duur zoals voorzien bij het ontwerp-Kaderbesluit en het

echter uitgegaan van de aanname dat de WBP eveneens van toepassing is op de verstrekking door telecommunicatieaanbieders en de bewaring in de situaties 2b en 3, nu immers bevragers pas de beschikking kunnen krijgen over de betreffende informatie in de in de wet omschreven (alsmede in het ontwerp-Kaderbesluit voorziene) situaties.

5.5.2 Overige wetgeving

Daarnaast is relevant de Telecommunicatiewet, in het bijzonder de hoofdstukken 11 en 13, in verband met de bewaring en verstrekking van gegevens betreffende abonnees (hieronder kunnen, in tegenstelling tot de WBP, zowel natuurlijke als rechtspersonen vallen).

Relevant zijn verder met name:

- Artikel 10 van de Grondwet, dat inbreuk op het recht op bescherming van de persoonlijke levenssfeer mogelijk maakt voor zover deze inbreuk plaatsvindt 'bij of krachtens de wet'.

- Artikel 15 van Richtlijn 2002/58[40], waarin een artikel is opgenomen op grond waarvan een bewaarplicht kan worden ingevoerd voor de in het ontwerp-Kaderbesluit omschreven doeleinden. Volgens artikel 15 kunnen de lidstaten wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de genoemde redenen (om onderzoek naar strafbare feiten mogelijk te maken of de openbare veiligheid, defensie en staatsveiligheid te beschermen). Alle in dit kader genomen maatregelen dienen volgens hetzelfde artikel echter wel in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht.

- Het Databeschermingsverdrag van de Raad van Europa van 28 juni 1981[41]. Relevant is artikel 9 van het Databeschermingsverdrag. Blijkens dit artikel is een verwerking van persoonsgegevens voor een ander doel mogelijk, indien dit bij *wet* is voorzien en *noodzakelijk* is in een democratische samenleving *in het belang van het bestrijden van strafbare feiten*. De vergaring van de gegevens dient tevens rechtmatig te geschieden en dient niet bovenmatig te zijn, eisen die ook worden gesteld door de WBP.

---

ontwerp-Besluit vorderen gegevens telecommunicatie door de overheid c.q. door een TTP (opties 2b en 3) kan op grond van de Wet Politieregisters naar onze mening op dit moment op grond van par. 2 van de wet niet worden gerechtvaardigd. Er zal hiertoe dan (minstens) een toevoeging van een grond voor bewaring van gegevens van onverdachte personen zijn benodigd in art. 5a, zoals eveneens is geschied ten aanzien van het Register bedoeld in artikel 4 van de Wet melding ongebruikelijke transacties (art. 5a lid 1 onder b Wet Politieregisters). Het register zal echter (zoals art. 5a tevens eist) niet alleen worden gebruikt voor 'de strafrechtelijke handhaving van de rechtsorde', maar ook voor preventie. In deze grond is op dit moment niet voorzien; een algehele herziening van art. 5a zou voor de opties 2b en 3 dan ook zijn gewenst. Ook voor de situatie dat het register zou worden beheerd door een (publiekrechtelijke) dienst die geen organisatorische eenheid van de politie en/of de marechaussee is, maakt bewaring van gegevens in de gewenste vorm en omvang voor de opties 2b en 3 momenteel niet mogelijk is (art. 13c Wet Politieregisters), nog afgezien van de legitimiteitsvraag van de bewaring als zodanig in de situaties van de genoemde opties.

[40] Richtlijn 2002/58/EG van het Europees parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicati (richtlijn betreffende privacy en elektronische communicatie), PbEG 2002, L201.

[41] Verdrag tot bescherming van personen in verband met de geautomatiseerde verwerking van persoonsgegevens, 28 januari 1981, Trb. 1988, 7.

- Artikel 8 EVRM[42]. Artikel 8 EVRM staat eveneens een inbreuk op de persoonlijke levenssfeer toe wanneer daarin bij *wet* is voorzien en voor zover dit in een democratische samenleving *noodzakelijk* is in het belang van de in het belang van de nationale veiligheid, de openbare veiligheid, voor de bescherming van de openbare orde, gezondheid en goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

5.6 Bespreking optie 2a

In deze situatie ('het oorspronkelijke model van de overheidsinstantie') zal er effectief geen sprake zijn van bewaring door de overheid als verantwoordelijke in de zin van de WBP, doch blijven de gegevens onder verantwoordelijkheid van de telecommunicatieaanbieders zelf, terwijl de organisatie waar de gegevens worden bewaard fungeert als een bewerker in de zin van WBP. In zekere zin fungeert de organisatie hier als een soort overslagbedrijf, dat de gegevens bewaard ten behoeve van (en onder verantwoordelijkheid van) de telecommunicatieaanbieders, en dat vanuit deze opslag relevante gegevens in bepaalde wettelijk omschreven situaties mag doorgeleiden aan bevragers. Weliswaar zijn de gegevens door de bevragers snel en efficiënt benaderbaar, via een organisatie als de overheidsinstantie en via een door de overheid te beheren systeem van bevraging, doch de bevragers zelf zijn niet 'de eigenaars' van de informatie, evenmin als de bewarende organisatie. Bevragers kunnen pas over de gegevens beschikken in de wettelijk omschreven situaties, die bevraging legitimeren. Verstrekking door de telecommunicatieaanbieders in de zin van de WBP vindt pas plaats op het moment van bevraging, en dient derhalve te passen binnen de grenzen van bevraging[43].

Effectief behoeft in deze situatie derhalve niet de vraag te worden beantwoord of bewaring door de overheid wettelijk is toegestaan, daar bewaring plaatsvindt door de telecommunicatieaanbieders zelf, zij het dat dit is uitbesteed aan een organisatie als de overheidsinstantie.

Uitgaande van het bovenstaande dienen echter wel de volgende voorwaarden te worden gesteld aan deze situatie:

- De gegevens dienen door de bewerker daadwerkelijk zodanig te worden afgeschermd en beveiligd, dat deze inderdaad pas benaderbaar zijn na formele bevraging, via een centraal orgaan (zoals de overheidsinstantie), en slechts in de omvang en binnen de grenzen als toegestaan door de wet.

- De gegevens en het bewarings- en bevragingssysteem dienen zodanig te zijn afgeschermd en beveiligd, dat de gegevens niet door anderen dan rechtmatige bevragers kunnen worden bevraagd of ingezien.

- Nu de hierboven genoemde instantie een onderdeel van de overheid is, en tevens een functie vervult ten aanzien van bevragende instanties, dient er effectief en democratisch toezicht en

[42] Verdrag van 4 november 1950 tot bescherming van de rechten van de mens en de fundamentele vrijheden, Trb. 1951, 154 en Trb. 1990, 156, laatstelijk gewijzigd bij het protocol van 11 mei 1994, Trb. 1994, 141 en 165.
[43] Nogmaals: deze grenzen zijn geen onderwerp van dit onderzoek.

controle te (kunnen) worden uitgevoerd op naleving van het bovenstaande, bij voorkeur door een onafhankelijk toezichthoudend orgaan.

5.7 Bespreking optie 2b

In deze situatie worden de volledige bestanden met de te bewaren gegevens na verstrekking door telecommunicatieaanbieders door de overheid zelf bewaard (en geraken zij dus uit de macht en verantwoordelijkheid van de telecommunicatieaanbieders). Verstrekking van gegevens door de telecommunicatieaanbieders vindt dan reeds plaats op het moment van overdracht, niet pas op het moment van bevraging.

Voor de systematische overdracht van gegevens voor dit doeleinde is momenteel geen basis in de WBP te vinden. Artikel 8 voorziet niet in een bruikbare grond voor deze verwerking[44]:

- Artikel 8 a, b en d zijn niet van toepassing.
- Artikel 8 c niet: er is geen bestaande wettelijke verplichting voor telecommunicatieaanbieders om grootschalig gegevens over te dragen aan de overheid.
- Evenmin artikel 8 e: weliswaar is de verstrekking nuttig voor de vervulling van de taak van legitieme bevragers, doch dit doel kan ook op andere wijze worden bereikt, namelijk door bevraging bij bewarende telecommunicatieaanbieders zelve. Verstrekking ter bewaring door de overheid is niet noodzakelijk voor de taakuitvoering.
- En ook het restartikel 8. f niet: deze ‘vergaarbak’ kan naar onze mening niet worden gebruikt om een zo ingrijpende overdracht van gegevens te rechtvaardigen, zonder verdere wettelijke fundamentering. Bovendien zouden de gegevens niet in het belang van de derde (het betreffende overheidsorgaan) worden verstrekt, maar in het belang van de legitieme bevragers.

Uitgaande van het feit dat de te verstrekken gegevens waren vergaard door de telecommunicatieaanbieders voor een ander doel dan voor verstrekking aan de overheid ter bewaring[45], dient verder nog te worden gekeken naar art. 9 WBP. De vraag is of volgens de wet het doel van de beoogde verstrekking verenigbaar is met de doeleinden waarvoor de gegevens waren verkregen. De (niet-limitatieve) criteria voor beoordeling daarvan (artikel 9 lid 2) sluiten naar onze mening de onderhavige beoogde verstrekking uit. Bovendien laat dit artikel de aanbieder vrijheid een andere keuze te maken dan te verstrekken aan de overheid, waardoor het doel (grootschalige bewaring voor centrale en efficiënte bevraging) mogelijk niet zal worden gehaald.

[44] In de Telecommunicatiewet zijn de gronden en grenzen voor verwerking van verkeersgegevens, nummergegevens en locatiegegevens te vinden in art. 11.5, 11.5a en 11.9. Ook deze bieden geen grond voor verstrekking in de zin van optie 2b.
[45] Immers: uitgangspunt voor het onderhavige onderzoek is dat de gegevens toch al beschikbaar zijn bij de aanbieders, in lijn met het genoemde Stratix-rapport.

Artikel 43 WBP biedt de telecommunicatieaanbieder nog wel de mogelijkheid de afweging van artikel 9 uit te sluiten, voor zover dit noodzakelijk is in het belang van: (gronden opgenomen voor zover relevant, AMK) de veiligheid van de staat en de voorkoming en vervolging van strafbare feiten[46]. Dit artikel impliceert echter telkens een afweging van de verantwoordelijke aanbieder zelf of hij bepaalde gegevens zal verstrekken, geen verplichting tot verstrekking. Voor systematische bewaring van verkeersgegevens door de overheid is dit artikel dan niet voldoende. Bovendien is het niet *noodzakelijk* voor de genoemde belangen dat de gegevens worden bewaard door de overheid; ook hier zou bevraging van de aanbieders door de legitieme bevragers voldoende kunnen zijn voor uitvoering van de taken. Voorafgaande grootschalige opslag van verkeersgegevens bij de overheid is daarvoor geen noodzakelijke voorwaarde, hooguit een efficiënte voorwaarde.[47]

Op grond van de huidige wetgeving kan bewaring door de overheid derhalve niet worden geconstrueerd, omdat deze naar onze mening reeds afspringt op de onmogelijkheid[48] voor telecommunicatieaanbieders om de gegevens op de voorgestelde grootschalige wijze te verstrekken voor het genoemde doeleinde. De conclusie moet zijn dat voor de invoering van optie 2b een wetswijziging noodzakelijk zal zijn.

Een ander, gerelateerd argument tegen overdracht aan en opslag onder verantwoordelijkheid van een overheidsorgaan zelve is nog het volgende. Voor de verstrekking van verkeersgegevens ten behoeve van bevraging is reeds c.q. wordt regelgeving voorbereid, die strikt omschrijft door welke politiële/justitiële instantie of inlichtingendienst in welke gevallen welke informatie mag worden opgevraagd van telecommunicatieaanbieders. De situatie zou bevreemden, indien voor een dergelijke grootschalige overdracht van verkeersgegevens (ook van niet-verdachten) aan een overheidsorgaan ter bewaring voor bevragingsdoeleinden geen zodanige specifieke wetgeving noodzakelijk zou zijn, maar zou kunnen worden volstaan met de algemene bewoordingen van de WBP dan wel de Telecommunicatiewet. Weliswaar is het betreffende overheidsorgaan evenzo gebonden aan de wettelijke normen en waarborgen terzake van bevraging van de gegevens door de politie, justitie en inlichtingendiensten. De bewaring bij het orgaan op zichzelf dient echter naar onze mening geen doel dat noodzakelijk is voor deze bevraging, nu dit ook op andere wijze kan worden opgelost. Ook is het zaak iedere schijn van mogelijke belangenverstrengeling te voorkomen, hetgeen in een situatie dat de gegevens rechtstreeks door de overheid worden bewaard, opgeschoond en verstrekt minder eenvoudig zal zijn dan in de situatie dat de gegevens onder verantwoordelijkheid blijven vallen van de telecommunicatieaanbieders zelf.

Ook indien zou worden geconcludeerd dat grootschalige verstrekking door telecommunicatieaanbieders aan de overheid ter bewaring van de verkeersgegevens door de overheid wèl mogelijk zou zijn, is deze optie 2b naar onze mening momenteel niet haalbaar. Er is niet voldaan aan het noodzakelijkheidscriterium van het EVRM alsmede van het Databeschermingsverdrag.

[46] Een vergelijkbaar artikel kan gevonden worden in art. 11.13 van de Telecommunicatiewet. Ook dit artikel impliceert een afweging door de telecommunicatieaanbieder.
[47] En wellicht ook wel voor de aanbieders zelf efficiënt, immers eigen opslag voor bevraging zal investering in systemen vergen!
[48] En wellicht ook de onbereidheid, waardoor het beoogde doel van grootschalige opslag en efficiëntie niet wordt bereikt.

De bewaring door de overheid is niet *noodzakelijk* voor de uitvoering van de taken van bevragers, hooguit efficiënt.

NB Deze situatie zou mogelijk anders zijn indien de gegevens gecodeerd en/of geanonimiseerd zouden worden verstrekt, waarbij pas op het moment van bevraging ontsleuteling en/of personalisering plaats zou vinden bij het overheidsorgaan (al dan niet met tussenkomst van de aanbieder of een onafhankelijke derde die de sleutel tot decodering en/of personalisering beheert).
De vraag is uiteraard of dit haalbaar is, en of dit voor alle verkeersgegevens mogelijk is. Wellicht zou hiermee kunnen worden bereikt dat de opslaglast van aanbieders wordt verminderd, terwijl de bevraging van de gegevens kan worden beheerst doordat dit slechts zal kunnen als de bevrager de beschikking krijgt over de decodering. Dezelfde eisen zouden dan moeten worden gesteld aan het ontsleuteling/personaliseringsproces als hierboven gesteld ten aanzien van situatie 2a.

5.8 Bespreking optie 3

Naar onze mening zal voor optie 3 eenzelfde redenering dienen te gelden als voor optie 2b. Deze optie is momenteel derhalve geen mogelijkheid. Mogelijk zou dit weer anders zijn in geval van codering / anonimisering als beschreven bij optie 2b.

5.9 Haalbaarheid van de opties

Uitgaande van het feit dat een bewaarplicht als hierboven bedoeld zal worden geïmplementeerd, is optie 2a, de situatie vergelijkbaar met het oorspronkelijke model en systeem van de overheidsinstantie, op grond van de huidige wetgeving naar onze mening een mogelijke optie. Effectief behoeft in deze situatie eigenlijk niet de vraag te worden beantwoord of bewaring door de overheid wettelijk is toegestaan, daar bewaring plaatsvindt door (onder verantwoordelijkheid van) de telecommunicatieaanbieders zelf, zij het dat de daadwerkelijke bewaring is uitbesteed aan een instantie als de overheidsinstantie (waarbij deze instantie als bewerker is aan te merken).

Er dient voor deze situatie echter wel aan een aantal voorwaarden te worden voldaan:

- De gegevens dienen door de bewerker daadwerkelijk zodanig te zijn afgeschermd en beveiligd, dat deze inderdaad pas benaderbaar zijn na formele bevraging, via een centraal orgaan (zoals de overheidsinstantie), en slechts in de omvang en binnen de grenzen als toegestaan door de wet.

- De gegevens en het bewarings- en bevragingssysteem dienen zodanig te zijn afgeschermd en beveiligd, dat de gegevens niet door anderen dan rechtmatige bevragers kunnen worden bevraagd of ingezien.

- Op de functie ten aanzien van bevragende instanties dient er effectief en democratisch toezicht en controle te (kunnen) worden uitgevoerd op naleving van het bovenstaande, bij voorkeur door een onafhankelijk toezichthoudend orgaan.

Voor optie 2b, de situatie waarbij de verantwoordelijkheid voor de te bewaren gegevens al direct door de telecommunicatieaanbieders wordt overgedragen aan een overheidsorgaan, is momenteel geen basis in de WBP noch in de Telecommunicatiewet te vinden. Voor dit doeleinde kunnen de volledige gegevensbestanden door de telecommunicatieaanbieders momenteel niet systematisch aan een derde worden verstrekt. Indien voor deze optie wordt gekozen, impliceert dit een wetswijziging.

Ook indien anders zou worden geconcludeerd, is deze optie 2b naar onze mening momenteel niet haalbaar. Er is niet voldaan aan het noodzakelijkheidscriterium van het EVRM alsmede van het Databeschermingsverdrag. De bewaring van de volledige gegevensbestanden door en onder verantwoordelijkheid van de overheid, waarbij de gegevens formeel buiten de macht van de telecommunicatieaanbieders worden gebracht, is niet *noodzakelijk* voor de uitvoering van de taken van bevragers, hooguit efficiënt. Deze situatie zou mogelijk anders zijn indien de gegevens gecodeerd en/of geanonimiseerd zouden worden verstrekt (bijvoorbeeld met behulp van Privacy Enhancing Technologies, PET), waarbij pas op het moment van bevraging ontsleuteling en/of personalisering plaats zou vinden bij het overheidsorgaan (al dan niet met tussenkomst van de aanbieder of een onafhankelijke derde die de sleutel tot decodering en/of personalisering beheert). Dezelfde eisen zouden dan moeten worden gesteld aan het ontsleuteling/personaliseringsproces als hierboven gesteld ten aanzien van situatie 2a.

Zoals hierboven uitgelegd zal naar onze mening voor optie 3 een zelfde redenering dienen te gelden als voor optie 2b. Daarom behoort optie 3 momenteel niet tot de mogelijkheden.

6 Vervolgstappen

Verschillende relevante aspecten van de opslag en de bevraging van de historische verkeersgegevens zijn voor optie 1 en voor optie 2 hierboven uitvoerig aan de orde geweest. Na besluitvorming dienen vervolgstappen te worden geformuleerd teneinde de gekozen optie door te voeren. Hiervoor worden de onderstaande stappen voorgesteld.

6.1 Projectgroep

Een projectgroep dient in het leven te worden geroepen. Doel van deze groep is zorg te dragen voor de realisatie van de gewenste optie. De projectgroep identificeert de opdrachtgever, geeft de stakeholders aan en definieert de communicatiekanalen en de rapportagelijnen met deze 2 partijen, en stemt daarmee een overallplanning af. Deze groep dient tevens de onderstaande activiteiten te initiëren, te begeleiden en te monitoren.

6.2 Informatiebehoefte

De informatiebehoefte van de behoeftestellers is nog niet uitputtend bekend. In het Stratix-rapport zijn enkele type gegevens benoemd die door deze bevragers zijn gewenst. Gezien de recente dreigingen alsmede hun invloed op het veranderde karakter van de informatiebehoefte van de behoeftestellers en rekeninghoudend met het inmiddels verouderde Stratix-onderzoek (gestart in maart 2002 en afgerond in juni 2003), is het nodig de reeds geïnventariseerde informatiebehoefte te actualiseren en nader te detailleren. Specifieke focus dient daarbij onder meer te worden gelegd op de frequentie van de vraagstelling (oftewel werklast), de gewenste/geëiste responsetijd en de wijze van de aanbieding van de opgevraagde verkeersgegevens. Deze aspecten zijn van invloed op de inrichting van de daadwerkelijke ICT-oplossing die ten behoeve van de beschikbaarstelling van deze gegevens wordt gerealiseerd. Deze geactualiseerde informatiebehoefte geniet een hoge prioriteit aangezien deze in feite het uitgangspunt is voor de constructie van de gewenste oplossing.

De in de informatiebehoefte onderkende elementen (zoals de identiteit van de aansluiting bij de mobiele telefonie of identiteit van de bestemming bij de internettoegang) dienen te worden beschreven en vastgelegd. Deze beschrijvingen worden door de behoeftestellers goedgekeurd hetgeen als een fundament voor de oplossing wordt gebruikt die het mogelijk maakt de benodigde historische verkeersgegevens te kunnen opvragen. Hiermee wordt het tevens voor de behoeftestellers makkelijker in de opgeslagen gegevens te zoeken aangezien hiervoor gebruik wordt gemaakt van de informatie-elementen in plaats van de technische informatie.

6.3 Aanleveringproces

Nadat de informatiebehoefte van de behoeftestellers in kaart is gebracht, dient het proces voor de aanlevering van de verkeersgegevens door de telecommunicatieaanbieders te worden gestandaardiseerd. Dit nog te formaliseren aanleveringproces houdt het volgende in voor optie 1 en voor optie 2.

6.3.1 Optie 1

Voor deze optie dienen formele afspraken met de aanbieders te worden gemaakt omtrent de aanlevering van de gevraagde verkeersgegevens door de behoeftestellers. Het aanleveringsproces dient in dit geval onder meer aan te geven wat de geëiste aanbiedingswijze (elektronisch of papier) en de gewenste presentatievorm (lay-out & structuur) is, op welke wijze (e-mail of koerier) de gegevens worden aangeboden, wat de geëiste responsetijd is en welke rapportage- en communicatiestructuur wordt gehanteerd. Eveneens wordt aandacht geschonken aan de manier waarop de beveiliging van de aan te leveren gegevens wordt geregeld.

6.3.2 Optie 2

Additionele afspraken gelden voor deze optie aangezien de verkeersgegevens ten behoeve van de opslag en bevraging worden aangeleverd. Naast de hierboven genoemde aspecten dienen onder andere afspraken te worden gemaakt en in het aanleveringproces te worden beschreven omtrent de benodigde gegevens om te kunnen voldoen aan de informatiebehoefte van de behoeftestellers, de gewenste frequentie van de aanlevering (bijvoorbeeld dagelijks, wekelijks), de locatie waar de aan te leveren verkeersgegevens worden klaargezet, en over de controles teneinde een adequate transmissie van deze gegevens alsmede de volledigheid hiervan te kunnen waarborgen.

6.4 Impactanalyse

De invloed van de beschikbaarstelling van de gewenste/geëiste historische verkeersgegevens en de hieraan te stellen eisen en wensen (zoals responsetijd en de aanbiedingswijze) op de organisatorische processen en op de technische infrastructuur dient voor optie 1 en voor optie 2 exact te worden onderzocht. Deze impactanalyse geeft eveneens de succesfactoren aan en identificeert de mogelijke risico's.

Nadat inzicht is verschaft in de bovenstaande organisatorische en technische gevolgen, worden de bijbehorende kosten in kaart gebracht. Hiervoor kunnen de externe leveranciers worden benaderd, waarvoor de volgende werkwijze wordt voorgesteld. Met behulp van de zogeheten 'Request For Information' procedure wordt een aantal leveranciers benaderd om informatie te verstrekken omtrent hun werkwijze teneinde te voldoen aan de gewenste organisatorische of technische verandering en/of vernieuwing. Op basis van de beschikbaargestelde informatie worden enkele leveranciers benaderd om een zogeheten 'pre-proposal' uit te brengen aan de hand waarvan zij een prijsindicatie geven van de te verwachten kosten.

6.4.1 Optie 1

Bij deze optie dient gedurende de impactanalyse aandacht te worden geschonken aan de architectuurvorm die de telecommunicatieaanbieders van plan zijn te realiseren ten behoeve van de opslag en bevraging van de historische verkeersgegevens. Dit inzicht is relevant voor een adequate aansluiting met de door de behoeftestellers gewenste functionaliteit. Tevens is het nodig rekening te houden met de eventuele impact van deze werkwijze op de besturing van het opslag- en bevragingproces bij de telecommunicatieaanbieders.

6.4.2 Optie 2

Gezien de bekendheid met de overheidsinstantie kan voor optie 2 worden volstaan met de algemene impactwerkzaamheden, zoals hierboven genoemd. De gewenste organisatievorm dient tevens te worden gekozen, zodat er helderheid is omtrent de toekomstige architectuur van optie 2.

6.5 Activiteitenplanning en doorlooptijd

Op basis van de uitkomsten van de impactanalyse dienen de verwachte werkzaamheden te worden ingedeeld in stappen die gefaseerd worden uitgevoerd. Per fase wordt de bijbehorende planning gemaakt en de benodigde mensen en middelen ingepland.

6.6 Realisatie

Voor de realisatie van de daadwerkelijke ICT-oplossing om de historische verkeersgegevens aan te bieden, kan worden overwogen of dit traject wel of niet dient te worden uitbesteed. Uit de praktijk blijkt dat er een beperkt aantal leveranciers is dat de mogelijkheden, faciliteiten en de benodigde kennis en ervaring heeft om omvangrijke gegevenscapaciteiten te ontwikkelen. Het is derhalve noodzakelijk door middel van een zorgvuldig selectieproces een leverancier te zoeken. De in de vorige stap benaderde leveranciers kunnen logischerwijs bij dit proces worden betrokken.

7 Marktontwikkelingen

De opslag en het toegankelijk maken van gegevens op een efficiënte wijze heeft thans veel aandacht. Organisaties in uiteenlopende sectoren slaan diverse soorten gegevens op als gevolg van hun businessoperaties. Deze opslag vindt normaliter plaats in verschillende systemen en is meestal moeilijk benaderbaar. Voortdurend wordt gezocht naar oplossingen om deze decentrale gegevens toegankelijk te maken, zodat de gewenste informatie middels bevragingen kan worden verworven.

Voor de opslag en de bevraging van gegevens zijn door leveranciers verschillende concepten geïntroduceerd. Een voorbeeld hiervan is een concept voor het verzamelen van logs en voor het opslaan van deze bestanden gebruikmakend van compressietechnieken dat niet lang geleden op de markt is gelanceerd. Op de opgeslagen gegevens worden vervolgens indices gemaakt om de toegankelijkheid te vergroten. Als gevolg hiervan kan de bevraging op een efficiëntere wijze geschieden. Voor een nader inzicht in dergelijke oplossingen zijn interviews gehouden met één leverancier. Volgens zijn mededeling kan circa 70% besparing worden gerealiseerd op de opslagcapaciteit. Dit wil concreet zeggen dat een log van 1TB een opslagruimte van 300GB in beslag neemt inclusief de indices. Met behulp hiervan wordt de opgeslagen log bevraagd om de gewenste informatie op te vragen, waardoor een snellere responsetijd kan worden gerealiseerd. Volgens de leverancier kost een stand-alone model met een opslagcapaciteit van 300GB circa $34.000,-. Dit model kan worden uitgebreid met 1TB en 3TB modules die respectievelijk $20.000,- en $35.000,- kosten.

Een ander voorbeeld van een geavanceerd opslagsysteem is het nieuwe topmodel van een gerenommeerde hardwareleverancier. Recentelijk heeft deze internationale en in de industrie bekende leverancier de opslagsystemen gepresenteerd die aanmerkelijk kleiner en sneller zijn, en meer schijfruimte bieden dan de huidige apparatuur. Deze nieuwe opslagmachine heeft glasvezel-interconnecties en biedt de uiteindelijke maximale capaciteit van 96PB. Uitbreiding vindt plaats door middel van modules met elk 16 schijven met een capaciteit van 73, 146 en 300GB. Het opslagsysteem ondersteunt verbindingen naar mainframes en open omgevingen en bezit een beschikbaarheid van 99.9999 procent. Een prijsindicatie van dit systeem is niet gegeven.[49]

[49] Bron: Computable, 22 oktober 2004, 37e jaargang, nummer 43.

A Documentatie en interviews

In deze bijlage zijn de bestudeerde documentatie en geïnterviewde medewerkers gepresenteerd.

A.1 Documentatie

De hieronder genoemde documentatie is voor dit onderzoek beschikbaar gesteld en bestudeerd:

- Blarkom, G.W. van, en J.J. Borking, Beveiliging van persoonsgegevens: Achtergrondstudies en Verkenningen 23, Registratiekamer, Den Haag, april 2001.
- Council Of The European Union, COPEN 77 TELECOM 125, 10767/04, 25 June 2004.
- Council Of The European Union, CRIMORG 36 TELECOM 82, 8958/04, 28 April 2004.
- Deloitte & Touche, Rapportage onderzoek justitiële kosten telecommunicatie ten behoeve van Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, december 2002.
- Directie Informatisering, Basisvoorzieningen Informatiebeveiliging Ministerie van Justitie, versie 1.0 definitief, 8 maart 2000.
- Directoraat-Generaal Telecommunicatie en Post, Regeling aftappen openbare telecommunicatienetwerken en –diensten, 30 mei 2001.
- Interpol Expert Statement, European Working Party on Information Technology Crime.
- KPN, Jaaroverzicht en samenvatting financiële gegevens, 2003.
- KPN Persberichten, KPN sluit succesvol kwartaal af met een winst na belastingen van EUR 375 miljoen, Den Haag, 10-05-2004.
- Ministerie van Justitie, Besluit vorderen gegevens telecommunicatie.
- Raadswerkgroep COPEN (Justitiële samenwerking), Verslag, 4 juni 2004.
- Staatsblad van het Koninkrijk der Nederlanden, Besluit beveiliging gegevens aftappen telecommunicatie, jaargang 2003.
- Stratix, Onderzoek ‘Bewaren Verkeersgegevens door Telecommunicatieaanbieders’, juni 2003.

- TNO Strategie, Technologie en Beleid, Netwerken in cijfers 2004: Trendrapportage ICT-infrastructuur en diensten, 9 juni 2004.
- Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie, maart 2004.

A.2 Interviews

Tijdens dit onderzoek is overleg gevoerd met de volgende functionarissen:

Functie	Organisatie
Directeur overheidsinstantie	Overheid
Hoofd Bureau PIDS	Ministerie van Justitie
Programma Manager bij overheidsinstantie	Extern
Beleidsmedewerker	Ministerie van Binnenlandse Zaken & Koninkrijksrelaties
Consultant bij de overheidsinstantie	Extern

Tevens zijn gesprekken gevoerd met enkele hardware- en softwareleveranciers.

B Afkortingen

De in dit rapport gebruikte afkortingen zijn hieronder opgesomd:

ACTAL	Adviescollege Toetsing Administratieve Lasten
ADSL	Asymmetric Digital Subscriber Line
CCTA	Central Computer and Telecommunications Agency
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
CRAMM	CCTA Risk Analysis and Management Method
DHCP	Dynamic Host Configuration Protocol
GB	Gigabyte (10^9 bytes)
IBVA	Informatiebeveiligingsambtenaar
IP	Internet Protocol
ISP	Internet Service Provider
MB	Megabyte (10^6 bytes)
PET	Privacy Enhancing Technologies
PB	Petabyte (10^{15} bytes)
PIDS	Platform Interceptie, Decryptie en Signaalanalyse
POP3	Post Office Protocol version 3
RADIUS	Remote Access Dial In User Service
SG	Secretaris Generaal
SMTP	Simple Mail Transfer Protocol
SAN	Storage Area Network
TB	Terabyte (10^{12} bytes)
TTP	Trusted Third Party

UDP	User Datagram Protocol
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie
WBP	Wet Bescherming Persoongegevens