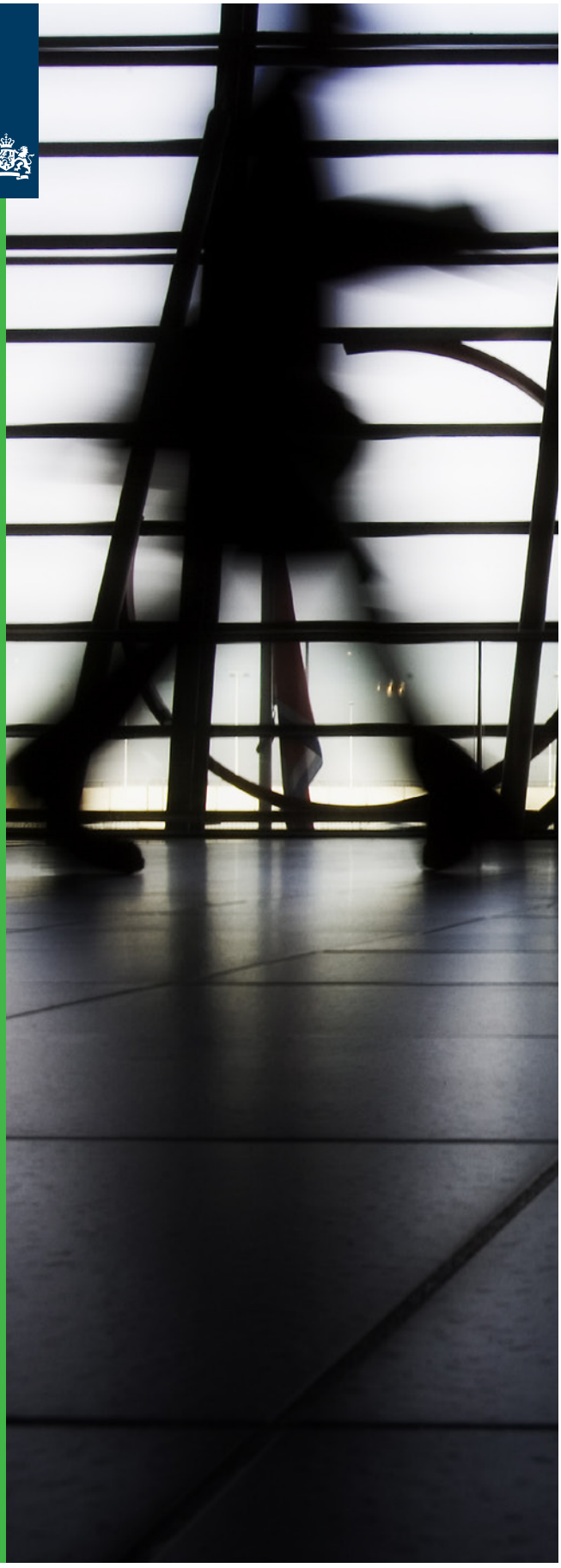
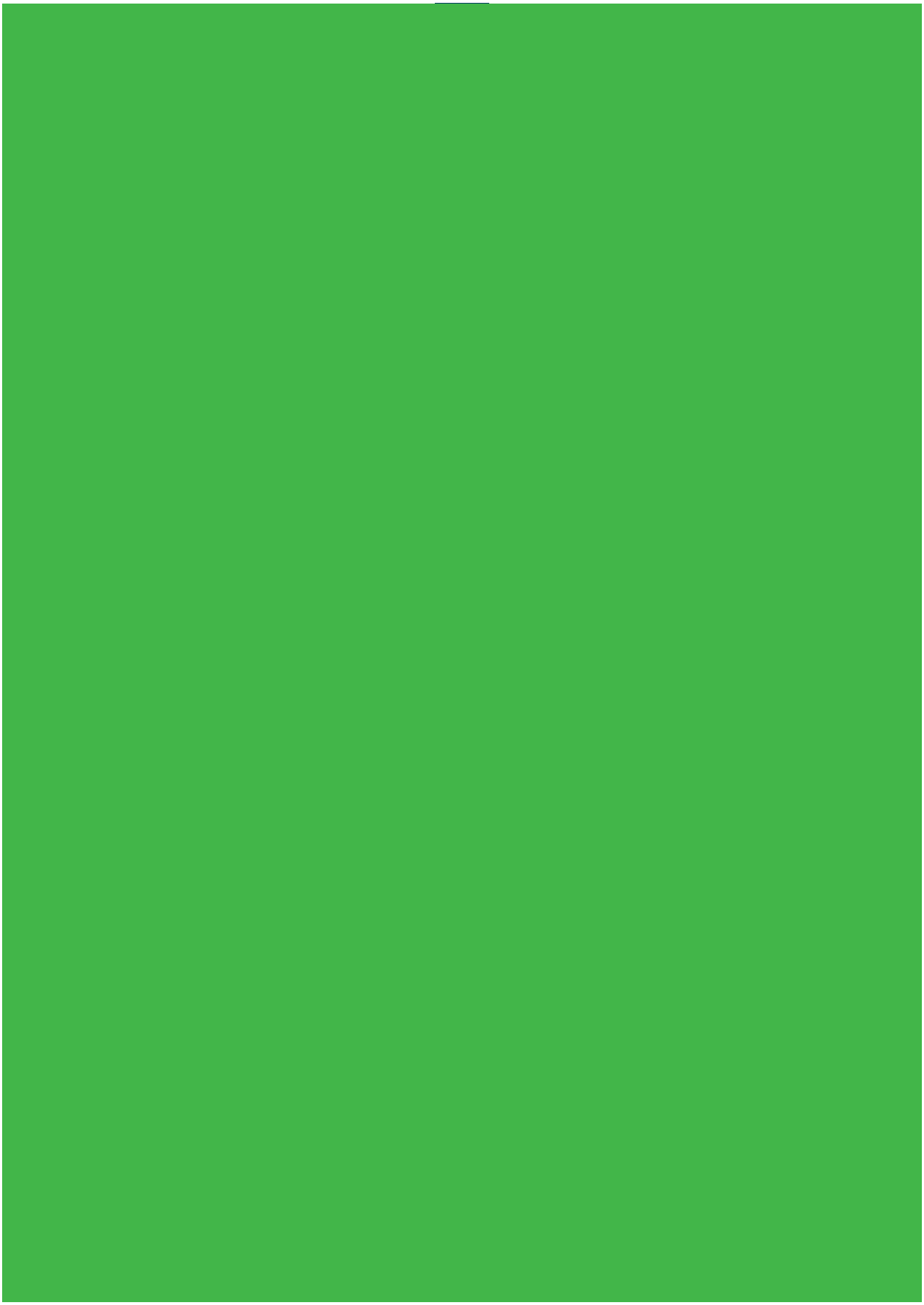
# Digitale spionage

Wat is het risico?





# Digitale spionage

## Wat is het risico?

Digitale spionage is steeds vaker een onderdeel van ongewenste activiteiten van buitenlandse inlichtingendiensten. Ook andere actoren, zoals bedrijven, kunnen gebruik maken van dergelijke activiteiten, die de nationale veiligheid beschadigen. Hierbij kan het gaan om belangen op het terrein van territoriale, economische, ecologische en fysieke veiligheid en sociale of politieke stabiliteit. Vanwege de toename – ook mondiaal – is digitale spionage een actueel onderzoeksterrein van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Met deze brochure informeren de AIVD en de MIVD u over het werk van inlichtingendiensten. Ook leest u hoe u de risico's op digitale spionage kunt beperken.

**Loopt u risico?**
Inlichtingendiensten hebben interesse in politieke, geheime militaire, economische en wetenschappelijke informatie. Daarnaast is bekend dat een aantal buitenlandse inlichtingendiensten betrokken is bij manipulatie, beïnvloeding en het controleren van migrantengroepen in ons land. Zij zetten hierbij digitale spionage in om gegevens te bemachtigen van organisaties die zich bezighouden met belangenbehartiging van migrantengroepen. Zij zijn bijvoorbeeld geïnteresseerd in beleidsplannen of ledenlijsten.

Beoordeel zelf of u vanuit uw functie of privéleven risico loopt op spionage; bedenk of u beschikt over interessante kennis of dat u zich in een positie bevindt die interessant is voor buitenlandse inlichtingendiensten. Vaak weet u meer dan u in eerste instantie denkt.

**Doelwit: ambassades, ministeries en internationale instellingen**
In 2009 bleek dat het spionagenetwerk GhostNet honderden ambassades, ministeries en internationale instellingen hackte. GhostNet hackte via gerichte e-mails met geïnfecteerde Word- en pdf-bestanden. Zodra een computer geïnfecteerd was, kopieerde GhostNet de documenten en luisterde gesprekken af via webcams en microfoons. GhostNet werd aangestuurd met computers die bijna allemaal leidden naar China.

# Hoe werken inlichtingendiensten?

Digitale spionage vindt meestal plaats via installatie van spyware op een computer. Spyware is software die informatie vergaart van een computer, zonder dat de gebruiker van die computer dit weet. De informatie wordt dan ongemerkt naar de 'aanvaller' verzonden. Spyware kan toetsaanslagen registreren, het netwerk doorzoeken, een mailbox doorzoeken, screenshots maken et cetera. Er zijn zelfs gevallen bekend waarbij spyware ingezet wordt voor het afluisteren en bekijken van beelden. Daarvoor worden aanwezige microfoons en webcams gebruikt.

Spyware wordt op verschillende manieren geïnstalleerd. Hieronder leest u de meest voorkomende methoden.

### Via e-mail trojans

E-mail trojans zijn e-mailberichten met een besmette bijlage. Als u de bijlage opent, wordt uw computer geïnfecteerd met spyware. Bij gerichte digitale spionage probeert de aanvaller het mailbericht optimaal af te stemmen op de geadresseerde(n) en zijn werkzaamheden. De aanvaller wekt hierbij de schijn dat het bericht van een andere, bekende bron afkomstig is. Dit noemen we 'e-mail spoofing'. De kwetsbaarheden in de software zijn in de meeste gevallen bekend. Maar helaas ontdekken virusscanners e-mail trojans nog niet altijd.

### Via besmette websites

Een bezoek aan een website kan leiden tot installatie van spyware op uw computer. Hiervoor gebruiken de aanvallers een lek in de browser of een lek in de extra geïnstalleerde software (plug-ins) voor de browser, zoals flashspelers. De aanvaller kiest vaak een website die in de belangstelling staat van de doelwitten. De beheerder van de website merkt niets van de manipulatie. Het is ook mogelijk dat de aanvaller een website nabootst en vervolgens manipuleert. De aanvaller stuurt de doelwitten een e-mail die niet besmet is. Deze e-mail moet de doelwitten verleiden om naar de nagebootste site te gaan. Dit noemen we 'website spoofing'.

**Terwijl u nietsvermoedend het nieuws leest...**
Uw persoonlijke gegevens kunnen de hele wereld overgaan, vanaf het moment dat u een website bezoekt. Dat overkwam een aantal migranten toen zij een nieuwssite van hun migrantengemeenschap bezochten. De server van de nieuwssite was gehackt in opdracht van een buitenlandse overheid. De bezoekers van de website merkten hier niets van, maar hun persoonlijke gegevens werden via de gehackte server naar het spionerende land gestuurd. Deze persoonlijke gegevens kunnen in het betreffende land misbruikt worden om bijvoorbeeld familieleden van migranten onder druk te zetten.

### Via besmette media

Soms staat spyware al geïnstalleerd op media, voordat u deze gebruikt. Bijvoorbeeld op harde schijven, usb-sticks, cd's of dvd's. Door bijvoorbeeld usb-sticks gratis te verstrekken aan bepaalde groepen, is gerichte spionage mogelijk.

**Handig zo'n gratis usb-stick?**
Een topmanager bezoekt een conferentie over beveiliging. Bij een van de stands krijgt hij een usb-stick gratis. De volgende dag gebruikt hij die usb-stick op zijn werkplek. Helaas ... de usb-stick bevat spyware en zijn computer raakt besmet.


1 oo
2 abc
3 def
4 ghi
5 jkl
6 mno
mxyz

### Via spionage tijdens reizen

Tijdens reizen of verblijf in het binnen- en buitenland, bestaat het risico dat u uw laptop of andere gegevensdragers uit het oog verliest. U laat bijvoorbeeld uw laptop achter in uw hotelkamer of u moet deze tijdelijk afstaan bij de douane. Op deze momenten kunnen aanvallers spyware op uw laptop zetten of gegevens kopiëren. Ook wanneer u met uw laptop contact zoekt met een ogenschijnlijk veilige internetvoorziening in een publieke ruimte (bijvoorbeeld met een zogenaamde 'hotspot') bestaat het risico dat derden informatie proberen te verkrijgen.

**Blackberry even laten liggen**

Een hoge rijksambtenaar gaat beneden in zijn hotel een hapje eten en besluit zijn blackberry even te laten liggen in zijn hotelkamer. Een week later worden computers van het ministerie gehackt. De kans is groot dat onbekenden zijn hotelkamer zijn binnen gegaan en gegevens van zijn blackberry hebben gehaald.

# Wat kunt u doen?

Voor beveiliging bent u waarschijnlijk voor een deel afhankelijk van de ICT-afdeling van uw organisatie. Uw organisatie is verantwoordelijk voor een veilige, digitale werkomgeving. Daarnaast kunt u zelf ook de risico's van spionage beperken.

### In het algemeen

- Controleer altijd eerst het e-mailadres van een bericht. Twijfelt u over de legitimiteit van een e-mailbericht? Is het e-mailadres niet professioneel? Bijvoorbeeld: john1234@yahoo.com? Neemt u dan eerst contact op met de verzender om de authenticiteit te verifiëren. Open liever geen bijlagen van onbekenden, ook al lijkt de inhoud legitiem.

- Wees voorzichtig met het openen van bijlagen uit e-mails die u via een abonnement op een verzendlijst ontvangt. Aanvallers gebruiken soms verzendlijsten waarop u zich kunt abonneren. De afzender lijkt dan de reguliere verzender.

- Wantrouw e-mails met bijlagen die in slecht Engels gesteld zijn. Zeker als deze mail afkomstig is van een persoon die de Engelse taal goed zou moeten beheersen.

- Wantrouw e-mails die interessant zijn voor uw organisatie, maar niet voor u persoonlijk. Het is mogelijk dat de aanvallers slechts beschikken over uw e-mailadres en niet weten wat uw functie is.

**Een gevaarlijk abonnement**
Veel rijksambtenaren zijn geabonneerd op een nieuwsservice van de Europese Unie. Een aanvaller stuurt hen een e-mail met een geïnfecteerde bijlage. De e-mail lijkt afkomstig van de nieuwsservice van de Europese Unie. Dus openen de rijksambtenaren zonder te aarzelen deze geïnfecteerde bijlage.

- Wantrouw een bijlage als uw computer vreemd doet na het openen van die bijlage. Bijvoorbeeld als een applicatie opstart, afsluit, weer opstart en dan pas de bijlage opent en toont. Dit kan betekenen dat de bijlage besmet is.

- Wees voorzichtig met het achterlaten van uw e-mailadres op internet of op congressen, als u over gevoelige informatie beschikt. Wees ook voorzichtig met uw naam, want daarmee kunnen aanvallers uw e-mailadres gemakkelijk herleiden.

- Controleer usb-sticks en andere gegevensdragers met een scanner op een stand alone-pc. Of laat dit doen door uw helpdesk. Doe dit vooral als u een usb-stick gratis ontvangt of niet weet wat de herkomst van een usb-stick is.

- Creëer bewustzijn binnen uw organisatie voor de dreiging van digitale spionage.

### Als u thuis bent

- Zorg altijd voor een bijgewerkte virusscanner.
- Bewaar geen gevoelige, werkgerelateerde informatie op uw computer thuis.
- Wees u bewust van informatie die u op internet plaatst. Bijvoorbeeld op uw eigen websites, hyves, facebook et cetera. Hoe meer persoonlijke gegevens u op internet zet, hoe gemakkelijker het is om een gericht e-mailbericht samen te stellen.

### Als u op reis bent

- Zorg voor een minimale hoeveelheid (vertrouwelijke) data op uw gegevensdragers (laptops, usb-sticks, et cetera).
- Versleutel vertrouwelijke informatie als u die mee moet nemen.

**'Your laptop please ...!'**
Een zakenman reist voor zijn werk naar het buitenland. Bij binnenkomst moet hij meteen zijn laptop aan de douane afstaan. Drie uur later krijgt hij zijn laptop terug. Later vermoedt hij dat verschillende bestanden met concurrentiegevoelige bedrijfsinformatie zijn gekopieerd.

- Registreer vertrouwelijke informatie die u mee moet nemen. Zo kunt u eventueel achterhalen wat er in handen van derden is.
- Bewaar uw gegevensdrager in een verzegelde tas, wanneer u er zelf geen toezicht op kunt houden. Is de verzegeling verbroken? Of heeft u andere aanwijzingen om aan te nemen dat er gerommeld is met uw gegevensdrager? Gebruik de gegevensdrager dan niet meer.
- Voorkom het gebruik van aangeboden internet in openbare ruimten. Als een internetverbinding toch noodzakelijk is, verstuurt u dan geen vertrouwelijke informatie.

### Als u een vermoeden heeft

Vermoedt u dat het computernetwerk van uw organisatie doelwit is van digitale spionage? Laat dit dan weten aan de afdeling van uw organisatie die belast is met de beveiliging van de ICT-infrastructuur. Zij kunnen uw vermoeden bij de AIVD en de MIVD melden. Telefoonnummers en adressen vindt u achterin deze brochure. Uiteraard behandelen we uw melding uiterst vertrouwelijk.


home
pg up
pg dn
end

# Wat doen wij?

De taak van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) is:

*inlichtingenactiviteiten te onderkennen, te (helpen) beëindigen en de maatschappelijke weerstand ertegen te verhogen.*

Wees u bewust van het risico van spionage. Creëer ook bewustzijn binnen uw organisatie. Wilt u een melding over spionageactiviteiten of incidenten doen?
Dan horen we graag van u – ook wanneer u twijfelt.

# Wilt u meer weten?

Meer informatie leest u op de volgende sites:
- www.aivd.nl
- www.mivd.nl
- www.govcert.nl

Op www.aivd.nl en www.mivd.nl vindt u:
- de brochure ‘Spionage in Nederland. Wat is het risico?’
- de brochure ‘Spionage bij reizen naar het buitenland. Wat is het risico?’
- de jaarverslagen van de AIVD en de MIVD.

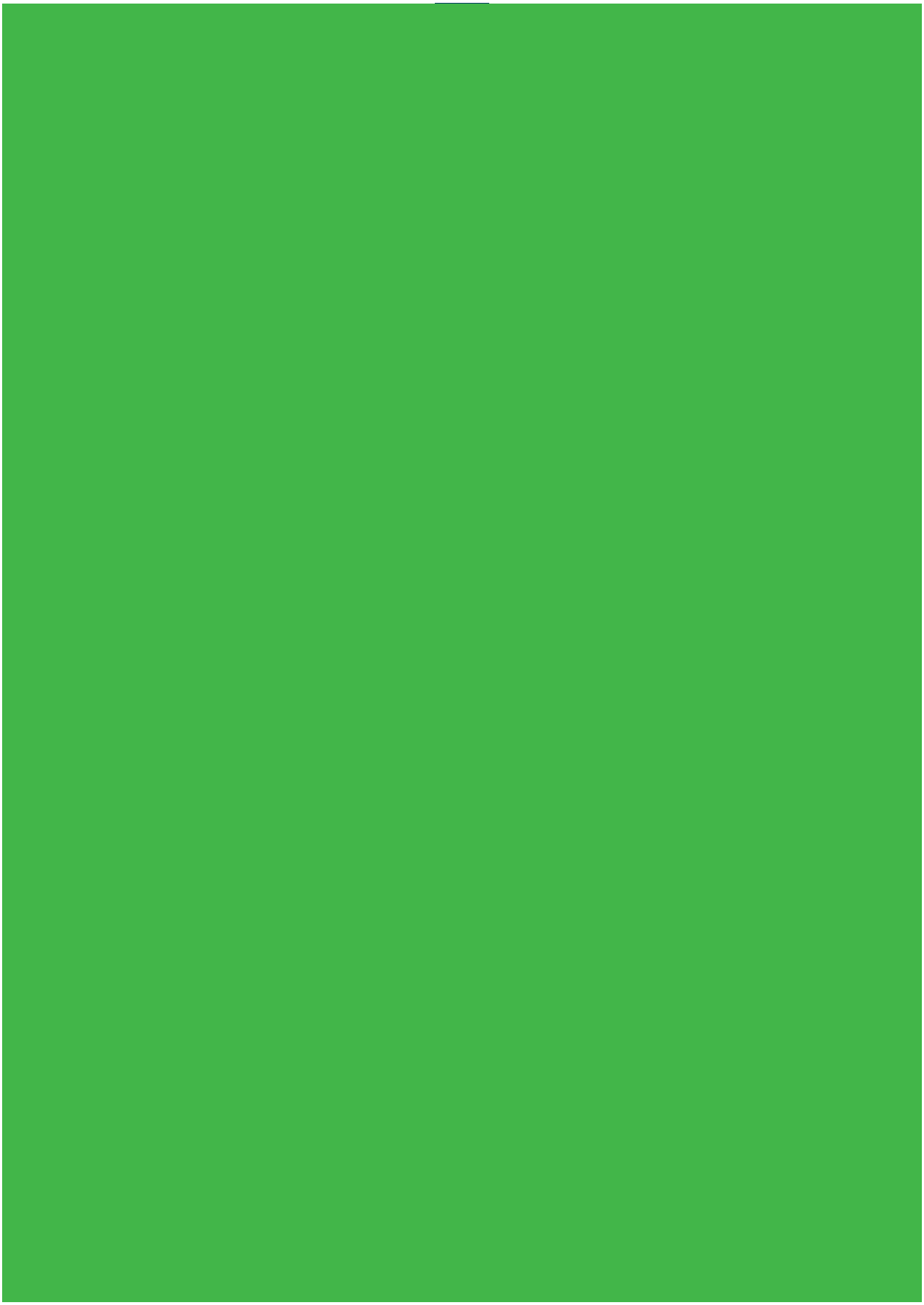
Heeft u vragen? Of wilt u een melding maken?
Neemt u dan contact met ons op. Onze adresgegevens zijn:

**Algemene Inlichtingen- en Veiligheidsdienst**

| | |
|---|---|
| Adres: | Postbus 20010 |
| | 2500 EA Den Haag |
| Telefoon: | 079 - 320 50 50 |
| Fax: | 070 - 320 07 03 |
| Website: | www.aivd.nl |

**Militaire Inlichtingen- en Veiligheidsdienst**

| | |
|---|---|
| Adres: | Postbus 20701 |
| | 2500 ES Den Haag |
| Telefoon: | 070 - 441 90 27 |
| Fax: | 070 - 441 90 10 |
| Website: | www.mivd.nl |



**Colofon**
Deze brochure is een uitgave van:

**Ministerie van Binnenlandse Zaken en Koninkrijksrelaties**
Algemene Inlichtingen- en Veiligheidsdienst
www.aivd.nl

Postbus 20010 | 2500 EA Den Haag

**Ministerie van Defensie**
Militaire Inlichtingen- en Veiligheidsdienst
www.defensie.nl/mivd

Postbus 20701 | 2500 ES Den Haag

**Grafische verzorging**
Zijlstra Drukwerk B.V., Rijswijk

1e druk, 2010

**Foto's**
Hollandse Hoogte

Januari 2010