

BESPIED ONS NIET

Geen twijfel meer mogelijk: we worden massaal bespioneerd door de NSA en GCHQ. Bovendien wil de Nederlandse regering zelf dit soort surveillance invoeren. Deze enorme inbreuk op de rechten van onverdachte Nederlanders moet stoppen.

Daarom eisen we dat onze regering alle nodige maatregelen neemt om haar burgers te beschermen en een einde te maken aan deze spionagepraktijken.

DECEMBER 2013



5 MAATREGELEN:

- 1. DE REGERING MOET IN KLARE TAAL DUIDELIJK MAKEN DAT MASSALE SPIONAGE NIET AANVAARDBAAR IS.**
- 2. DE REGERING MOET DE SCHAAL VAN DE SPIONAGE IN NEDERLAND ONDERZOEKEN.**
- 3. DE NEDERLANDSE GEHEIME DIENSTEN MOETEN WORDEN GECONTROLEERD EN AAN BANDEN WORDEN GELEGD.**
- 4. DE REGERING MOET HET GEBRUIK VAN BEVEILIGINGSTECHNOLOGIE BEVORDEREN.**
- 5. DE REGERING MOET IN EUROPA HARDERE MAATREGELEN EISEN.**

1. DE REGERING MOET IN KLARE TAAL DUIDELIJK MAKEN DAT MASSALE SPIONAGE NIET AANVAARDBAAR IS.

Veroordeel het bespioneren van onverdachte burgers.

Rutte moet deze schandalige inbreuken op de privacy van Nederlanders ten strengste veroordelen in een telefoongesprek met - en in een open brief aan - Obama. Frankrijk, Duitsland en andere landen namen al vergelijkbare stappen.

Roep de ambassadeur terug voor overleg.

Nederland moet direct zijn ambassadeur uit de Verenigde Staten terugroepen voor overleg en de Amerikaanse en de Engelse ambassadeur op het matje roepen. Voor deze onacceptabele inbreuk op de Nederlandse soevereiniteit die uitgaat van de Amerikaanse en Engelse surveillanceprogramma's zijn de strengste diplomatieke maatregelen op hun plaats.

Bevries grote lopende transacties met de VS.

De Nederlandse overheid overweegt grote orders aan te besteden bij Amerikaanse bedrijven, zoals de aanschaf van de JSF. Het benodigde vertrouwen voor deze orders is weg. Voor zover juridisch mogelijk moet de Nederlandse overheid deze deals bevriezen.

De regering moet deze schandalige inbreuken op de privacy van Nederlanders ten strengste veroordelen.

2. DE REGERING MOET DE SCHAAL VAN DE SPIONAGE IN NEDERLAND ONDERZOEKEN.

Onderzoek spionage bij bedrijven.

In Nederland zijn grote bedrijven gevestigd die een aantrekkelijk doelwit zijn voor de NSA of GCHQ. De NSA geeft jaarlijks 170 miljoen Euro uit aan het ondermijnen van beveiliging. De regering moet een instantie met voldoende bevoegdheden grondig laten onderzoeken of de Amerikaanse en Engelse geheime diensten deze bedrijven bespioneren of dat hebben gedaan. De resultaten daarvan moeten in een openbaar rapport naar het parlement worden gestuurd. Enkele suggesties:

- **NXP** maakt chips die gebruikt worden in de toegangspassen van de overheid en smartphones.
- **Fox-IT** is de leverancier van informatiebeveiliging van veel grote bedrijven in Nederland, de overheid én onze geheime diensten. Kunnen we sinds de hacks van de NSA er nog wel zeker van zijn dat hun systemen of mensen niet zijn gecompromitteerd?
- Alle telefoongesprekken in Nederland worden afgehandeld door een beperkt aantal aanbieders, zoals **KPN** en **Vodafone**. Het is niet onrealistisch dat de NSA heeft ingebroken op de systemen van deze aanbieders om toegang te krijgen tot het telefoonverkeer van Nederlandse burgers, politici en bedrijven. De NSA deed dat immers ook bij de Belgische aanbieder Belgacom.
- Ook **ABN** en andere Nederlandse banken moeten worden onderzocht. De afdeling "Follow the money" van de NSA hanteert het "maximum data collection"-principe en verzamelt alle financiële informatie waar zij haar handen op kan leggen. In door Snowden gelekte documenten wordt de

suggestie gewekt dat zij daarvoor heeft ingebroken op de systemen van SWIFT. Het is aannemelijk dat de NSA ook interesse heeft in Nederlandse banken.

- De **AMS-IX** is een van de grootste knooppunten voor uitwisselen van internetverkeer in de wereld en alle grote namen zijn er op aangesloten, waaronder ook Facebook en Google. Het is daarmee een interessant doelwit voor de NSA.
- De NSA bespioneert ook om economische belangen. Zo bleek ook de Braziliaanse oliegigant Petrobras te worden afgeluisterd. Het onderzoek moet zich daarom ook op **Shell** richten.

Onderzoek spionage bij politici en beleidsmakers.

We weten dat 35 regeringsleiders het doelwit zijn geweest van de NSA. Bovendien heeft de NSA instituties van de Europese Unie afgeluisterd. We moeten precies weten of ministers, topambtenaren en bestuursleden van relevante toezichthouders, zoals De Nederlandsche Bank, zijn afgeluisterd. Ook hierover moet publiek verantwoording worden afgelegd.

Onderzoek spionage op zeekabels.

De regering moet onderzoeken of de NSA of GCHQ de zeekabels aftapt die in Nederland uitkomen. Er komen zes internationale zeekabels met internetverkeer in Nederland uit. Ook hiervan moeten de resultaten worden gepubliceerd.

Onderzoek de naleving van de privacywet.

Het CBP moet onderzoeken of bij bedrijven die (mogelijk) doelwit zijn geweest van de NSA of

**We weten dat 35
regeringsleiders het
doelwit zijn geweest van
de NSA.**

**De regering wil een wet
introduceren die geheime
diensten de macht geeft
om op grote schaal
internetverkeer te
onderscheppen.**

GCHQ de Wet bescherming persoonsgegevens is overtreden.

Doe strafrechtelijk onderzoek naar spionage.

Het Openbaar Ministerie moet onderzoek doen naar strafrechtelijke overtredingen door de NSA en GCHQ. Het is strafbaar om vertrouwelijke communicatie af te luisteren. Als dit in Nederland is gebeurd, moeten de verantwoordelijken daarvoor worden vervolgd.

Bescherm klokkenluiders.

De regering moet klokkenluiders die waardevolle informatie geven over schending van grondrechten door geheime diensten, zoals het op grote schaal afluisteren van Nederlanders of andere mensen, bescherming bieden. Dat kan in de vorm van politiek asiel, strafrechtelijke immuniteit en waar nodig voorziening in hun levensonderhoud. Ook moeten uitleveringsverdragen worden aangepast zodat klokkenluiders niet hoeven te vrezen dat ze uitgeleverd worden.

3. DE NEDERLANDSE GEHEIME DIENSTEN MOETEN WORDEN GECONTROLEERD EN AAN BANDEN WORDEN GELEGD.

Trek de plannen voor een grootschalige af luisterbevoegdheid in.

De regering wil een wet introduceren die Nederlandse geheime diensten de macht geeft om op grote schaal en ongericht internetverkeer te onderscheppen. Dat is onacceptabel: we willen in Nederland geen NSA-achtige praktijken. Deze plannen moeten direct de prullenbak in.

Publiceer tapstatistieken Nederlandse geheime diensten.

De regering moet gaan publiceren hoe vaak onze geheime diensten Nederlanders hebben afgeluisterd. Dit hebben ze één jaar gedaan (na daartoe gedwongen te zijn door de Tweede Kamer), maar daarna zijn ze hiermee gestopt. Het moet duidelijk zijn hoeveel mensen worden afgeluisterd, hoe vaak gegevens worden gevorderd, welke databanken worden aangelegd en hoe hierop analyses zijn gedaan.

Maak het budget van geheime diensten transparanter.

Nu is vrijwel niet na te gaan wat de geheime diensten doen met overheidsgeld. In het jaarverslag van de geheime diensten moet volgens geaccepteerde jaarverslaggevingsbeginselen inzicht worden gegeven in de uitgaven van de geheime diensten. Onderdelen van het budget mogen geheim blijven, maar de cumulatieve omvang van deze onderdelen moet worden gemaximeerd op 1 procent van het totale budget van de geheime dienst.

Geheime diensten mogen geen informatie accepteren waarvan ze kunnen vermoeden dat deze is verkregen door schending van mensenrechten.

De CTIVD lijkt soms vooral woordvoerder van de geheime diensten.

Verbied geheime diensten besmette informatie te accepteren.

De geheime diensten mogen geen informatie accepteren van andere geheime diensten waarvan ze redelijkerwijs kunnen vermoeden dat deze is verkregen door schending van mensenrechten, inclusief informatie verzameld uit grootschalige, ongerichte surveillanceprogramma's. Dat betekent dat in ieder geval informatie die afkomstig is uit Prism (directe toegang bij Gmail, Facebook etc.), Upstream (grootschalig tappen van zeekabels door de NSA) of Tempora (grootschalig tappen van zeekabels door GCHQ) niet mag worden gebruikt. De geheime diensten moeten dus ook vragen naar de herkomst van gegevens als zij informatie toegeschoven krijgen.

Intensiveer het toezicht op de geheime diensten.

De voornaamste toezichthouder op de geheime diensten, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), lijkt soms vooral woordvoerder van onze geheime diensten. De huidige Commissieleden worden gekozen door de ministers die ook aan het hoofd van de geheime diensten staan. De CTIVD moet daarom vervangen worden door een écht onafhankelijke toezichthouder. De CTIVD moet worden geleid door bestuursleden die voor tenminste twee regeerperiodes zijn benoemd door de Tweede Kamer.

4. DE REGERING MOET HET GEBRUIK VAN BEVEILIGINGSTECHNOLOGIE BEVORDEREN.

Financier campagnes over cloudrisico's en encryptie.

De regering moet twee grootschalige en langdurige overheidscampagnes financieren die internetters bewust maken van massale internetspionage en maatregelen suggereren waarmee gebruikers zichzelf kunnen beschermen. Eén campagne moet gaan over het gevaar van het gebruik van decentrale oplossingen. De tweede campagne moet gaan over het gevaar en het gemak van het afluisteren van email en moet internetters adviseren om email te versleutelen.

Investeer in beveiligingstechnologie.

De regering moet een bedrag minstens even groot als 10 procent van het budget van de Nederlandse geheime diensten investeren in onderzoek naar en de ontwikkeling van cryptografie en anonimiseringstechnologie. Daarbij moet vooral worden geïnvesteerd in het verbeteren van de bruikbaarheid van bestaande technologie, zodat iedereen die technologie kan gaan gebruiken. Daarnaast moet worden geïnvesteerd in de ontwikkeling van software die het mogelijk maakt om versleuteld via de mobiele telefoon te bellen. Die technologie moet door onafhankelijke wetenschappers worden ontwikkeld en de broncode moet worden gepubliceerd onder een vrije en open softwarelicentie.

Nieuwe eis in aanbestedingen: broncode van software moet beschikbaar zijn.

De overheid moet als eis in aanbestedingen voor software opnemen dat de broncode beschikbaar wordt gesteld aan de overheid onder een vrije en open softwarelicentie. Waar nodig voert de

**Vooraf aan de
bruikbaarheid van
beveiligingstechnologie
kan nog veel worden
verbeterd.**

We weten nu niet hoe onze belangrijkste af luisterapparatuur werkt.

overheid audits op die software uit om te zien of achterdeuren zijn ingebouwd. Indien mogelijk publiceert de overheid de broncode onder een vrije en open softwarelicentie.

Maak audits van af luistertechnologie verplicht.

De Nederlandse politie en de geheime diensten moeten de broncode van hun eigen af luisterapparatuur en spyware krijgen zodat zij kunnen controleren of hierin achterdeuren zijn ingebouwd. Nog steeds gebruikt de Nederlandse overheid af luistertechnologie uit Israël, waarvan de werking niet precies te achterhalen is. Ondertussen zijn via een af luisterachterdeur in interceptietechnologie van Vodafone in Griekenland jarenlang politici afgeluisterd. Ook moet de overheid kunnen controleren dat de geleverde broncode daadwerkelijk wordt ingezet.

Versleutel verkeer waar mogelijk.

De Nederlandse overheid moet eisen dat verkeer tussen netwerkbeheerders vanuit Nederland waar mogelijk versleuteld wordt verstuurd. Dit betekent dus dat transitaanbieders en telecomaandbieders versleuteling aanzetten waar mogelijk.

Versleutel e-mailverkeer tussen servers.

Op dit moment wordt niet alle email tussen servers, bijvoorbeeld tussen Gmail en Yahoo, versleuteld verstuurd. Nederlandse e-mailaanbieders die onderling mail uitwisselen moeten dat versleuteld doen.

Versleutel verkeer naar overheidswebsites.

Alle overheidswebsites moeten hun websites versleuteld, dus met SSL/TLS, aanbieden. Op die manier wordt het moeilijker om verkeer te van burgers te onderscheppen.

Maak versleutelde communicatie met overheid mogelijk.

De overheid moet de mogelijkheid bieden om met haar instanties versleuteld te e-mailen met PGP/GPG en het gebruik hiervan stimuleren. Iedere ambtenaar krijgt een e-mailclient met mailencryptie en uitleg over het gebruik hiervan.

Verbied afname bespioneerde diensten door de publieke sector.

Alle overheidsdiensten, inclusief onderwijsinstellingen, moeten een garantie eisen van bedrijven waar ze persoonsgegevens opslaan dat deze gegevens niet aan buitenlandse veiligheidsdiensten worden afgestaan.

**De overheid moet de
mogelijkheid bieden om
versleuteld te e-mailen
met ambtenaren.**

**Er wordt al bijgehouden
wie we mailen, waar we
zijn, en wie we bellen op
grond van Europese
regelgeving.**

Schort onderhandelingen vrijhandelsverdrag met VS op.

De regering moet eisen dat de onderhandelingen tussen Europa en de Verenigde Staten over het vrijhandelsverdrag TAFTA worden opgeschort totdat zeker is dat de NSA en GCHQ niet meer op grote schaal Europeanen afluisteren. De VS onderhandelen nu met voorkennis, omdat zij weten wat de onderhandelingsruimte van Europa is.

Schaf privacy-uitzondering voor VS-bedrijven af.

De regering moet eisen dat de overeenkomst met de Verenigde Staten op grond waarvan gegevens over Europeanen door Amerikaanse bedrijven kunnen worden verzameld, de Safe Harbour Agreement, wordt beëindigd, omdat onze gegevens niet veilig zijn in Amerika.

Wissel niet langer financiële- en vluchtgegevens uit met Amerika.

De regering moet eisen dat Europese verdragen over de uitwisseling van persoonsgegevens van onverdachte burgers met de Verenigde Staten, zoals vlucht- en financiële gegevens, direct worden beëindigd. In ieder geval de PNR-overeenkomst en de SWIFT-overeenkomst moeten dus direct worden gestopt. Bilaterale verdragen met de Verenigde Staten op grond waarvan op grote schaal informatie wordt uitgewisseld, moeten worden gestopt.

Zet de bewaarplicht stop.

De regering moet eisen dat de richtlijn op grond waarvan precies wordt bijgehouden met wie en wanneer honderden miljoenen onverdachte Europeanen bellen en waar zij zijn direct wordt beëindigd. In Nederland moet de implementatie van deze richtlijn worden opgeheven.

Pleit voor Europese privacyregels om verzamelwoede aan banden te leggen.

De Nederlandse overheid moet in Brussel pleiten voor strengere Europese privacyregels, om zo de gegevensverzameling van Amerikaanse bedrijven - en de doorgifte van die gegevens aan de NSA - aan banden te leggen.

**De regering moet in
Brussel pleiten voor
strengere Europese
privacyregels, om zo de
doorgifte van gegevens aan
de NSA aan banden te
leggen.**