BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

**Post** Bits of Freedom
Postbus 10746
1001 ES Amsterdam

**Bank** 55 47 06 512
**KvK** 34 12 12 86

**M** +31(0)646282693
**E** simone.halink@bof.nl
**W** https://www.bof.nl

**Vaste commissie voor Veiligheid en Justitie**
**Tweede Kamer der Staten-Generaal**
**Binnenhof 4**
**2513 AA DEN HAAG**

**Betreft**
Commentaar op overheidsoptreden rondom Pobelka en het hackvoorstel

**Amsterdam**
23 mei 2013

Geachte leden van de Commissie voor Veiligheid en Justitie,

Tijdens het Algemeen Overleg Cybersecurity op woensdag 29 mei 2013 spreekt uw Commissie over de reactie van de minister op de berichtgeving van de NOS dat de overheid laks is geweest met betrekking tot het Pobelka-botnet en het onderzoek dat de minister naar dit botnet heeft laten verrichten.

De minister heeft zich op het standpunt gesteld dat de overheid in de Pobelka-casus adequaat heeft gehandeld.[1] Hij stelt dat de overheid meerdere middelen inzet om botnets zoals het Pobelka-botnet te bestrijden en dat in dit geval ook heeft gedaan. Daarnaast heeft hij nieuwe maatregelen aangekondigd die moeten helpen om botnets te bestrijden.[2]

Digitale burgerrechtenbeweging Bits of Freedom ziet reden om aan het standpunt van de minister en de noodzaak van de door hem aangekondigde maatregelen te twijfelen. Kort gezegd, is het optreden van de verantwoordelijke overheidspartijen en hun samenwerking gebrekkig gebleken. Van een noodzaak tot nieuwe – inbreukmakende – bevoegdheden kan in dat geval geen sprake zijn. Wij zullen deze punten hieronder toelichten en verzoeken u om deze mee te nemen in de voorbereiding van uw overleg.

1 O.a. TK 2012-2013, 26 643, nr. 268, p. 1.
2 *Idem*, p. 3 (Acties in de aankomende periode).

## 1. Inadequaat politie-optreden

Uit de feitelijke toelichting van de minister op de gebeurtenissen rondom Pobelka, waar kortheidshalve naar wordt verwezen[3], blijkt wel degelijk dat de overheid veel te laat in actie is gekomen. Team High Tech Crime (THTC) van de Landelijke Eenheid van de Politie heeft namelijk pas ruim een maand nadat zij bekend was geworden met het bestaan van de buitgemaakte dataset contact gezocht met het Nationaal Cyber Security Centrum (NCSC).

Het onderzoeksbureau Digital Investigation heeft de dataset in een vroeg stadium (16 oktober 2012) aan THTC aangeboden, maar THTC heeft Digital Investigation pas op 26 november 2012 met het NCSC in contact gebracht. In die tussentijd heeft THTC ervoor gekozen zelf geen nader onderzoek te verrichten omdat geen directe relatie kon worden gelegd met de uitbraak van het Dorifel-virus, waar door THTC al onderzoek naar werd gedaan. Dit terwijl zij wist dat de dataset informatie betrof die was buitgemaakt door een botnet dat een groot aantal Nederlandse bedrijven had getroffen en dat minstens één van de command & controlservers van dit botnet in Nederland stond.

Deze risico-inschatting van THTC is een verkeerde gebleken. Dit blijkt uit de handelingen die het NCSC in december 2012 heeft verricht, maar vooral uit de aanvullende actie die de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) 14 februari 2013 heeft genomen. Er is toen een grootschalig onderzoek gestart om de de potentiële impact van de gegevens in de dataset in te schatten. De NCTV partijen heeft daarbij partijen zoals het OM, de Politie, AIVD, MIVD en het NFI betrokken. Verder is een strafrechtelijk onderzoek opgestart.

Wanneer een overheidsdienst zoals THTC gegevens krijgt aangeboden waarvan de potentiële impact op de samenleving zo groot is, dan heeft zij de plicht direct een risico-analyse uit te voeren en in overleg te treden met de daarvoor aangewezen instantie. In het geval van Pobelka heeft zij dat verzaakt.

**Vraag:** Waarom heeft THTC toen zij met het bestaan van de dataset bekend werd niet direct een risico-analyse uitgevoerd en contact gezocht met het NCSC?

**Vraag:** Waarom was er voor THTC geen ruimte om af te wijken van lopend onderzoek? Immers, volgens de minister wordt "door de politie permanent onderzoek gedaan naar botnets".[4]

3 TK 2012-2013, 26 643, nr. 268 en nr. 272 inclusief bijlage; "Antwoord vragen van de leden Oosenbrug en Recourt over de reactie op een grote botnet-infectie door het Nationaal Cyber Security Centrum", TK 2012-2013, AH 2204; en "Antwoord vragen van het lid Gesthuizen over het bericht dat de overheid laks is geweest na een aanval door een botnet", TK 2012-2013, AH 2205.

**Vraag:** Wordt het inadequate optreden van THTC veroorzaakt door een gebrek aan capaciteit of kennis om een juiste risico-inschatting te maken? Zo ja, hoe wordt dit ondervangen?

**Vraag:** Waarom heeft THTC pas zo laat de hulp ingeroepen van NCSC? Hoe gaat de minister ervoor zorgen dat de verantwoordelijke partijen in de toekomst eerder en beter zullen samenwerken bij het inschatten van de risico's die uitgaan van botnets of vergelijkbare digitale dreigingen?

**Vraag:** Bent u het ermee eens dit zeer late politie-optreden niet bijdraagt aan de voorbeeldfunctie van de overheid op het gebied van cybersecurity en de urgentie die het onderwerp verdient?

## 2. Inadequaat optreden NCSC

Het NCSC is een onderdeel van het ministerie van Veiligheid en Justitie en daarbinnen van de NCTV. Terwijl de NCTV al eind november 2012 met de inhoud van de dataset bekend is geworden, heeft zij pas naar aanleiding van het media-aandacht op 14 februari 2013 reden gezien om gedegen onderzoek te doen naar de inhoud daarvan en daar andere partijen zoals het OM, de Politie, AIVD, MIVD en het NFI bij betrokken.

Deze gang van zaken is bijzonder kwalijk gezien de coördinerende rol van de NCTV en het belang van samenwerking in deze situatie, zoals de minister herhaaldelijk heeft benadrukt.[5] Deze samenwerking had er bijvoorbeeld toe kunnen leiden dat de doelgroep van het NCSC beter en eerder was geïnformeerd, ISPs en andere partnerorganisaties een grotere rol hadden gekregen bij het nemen van schadebeperkende maatregelen en dat reeds in een veel vroeger stadium strafrechtelijk onderzoek was gestart naar de criminelen achter het botnet. Het is onbegrijpelijk dat deze tekortkoming in het optreden van de overheid niet door de minister is geadresseerd.

**Vraag:** Hoe gaat de minister ervoor zorgen dat de NCTV in het geval van digitale dreigingen haar coördinerende rol voortaan naar behoren vervult?

**Vraag:** Hoe gaat de minister ervoor zorgen dat de samenwerking tussen verantwoordelijke partijen in het geval van digitale dreigingen wordt bevorderd? In het bijzonder, hoe gaat de minister ervoor zorgen dat er tussen verantwoordelijke partijen onderling beter over digitale

4 "Antwoord vragen van het lid Gesthuizen over het bericht dat de overheid laks is geweest na een aanval door een botnet", TK 2012-2013, AH 2205, antwoord op vraag 3.
5 O.a. TK 2012-2013, 260643, nr. 272, p. 2 (Acties op korte termijn).

dreigingen wordt gecommuniceerd?

Tegen deze achtergrond speelt ook de vraag of het NCSC over voldoende kennis en capaciteit beschikt voor de uitoefening van de haar toebedeelde taken. In zijn correspondentie over dit onderwerp onderstreept de minister diverse keren de belangrijke en centrale rol van het NCSC op het gebied van cybersecurity.[6] Uit zijn correspondentie blijkt echter ook dat bijvoorbeeld het informeren van de eigenaren van mogelijke getroffen informatiesystemen door het NCSC van haar een aanzienlijke inspanning vergt.[7] Dit is zorgelijk, want het is aannemelijk dat het belang en de omvang van de rol van het NCSC in de toekomst alleen maar zal toenemen.

**Vraag:** Hoe gaat de minister bij het NCSC in kennis en capaciteit voorzien die haar in staat stellen met deze centrale rol mee te groeien? Welk budget wordt hiervoor vrijgemaakt?

## 3. Aangekondigde maatregelen sluiten niet aan op directe behoefte

Uit de hiervoor in paragraaf 1 en 2 geschetste omstandigheden blijkt dat de taken en verantwoordelijkheden van het NCSC en de NCTV door andere partijen onvoldoende worden erkend. Dit geldt voor THTC, die pas na ruim een maand melding deed bij NCSC, maar ook voor haar doelgroep van Rijksoverheid en vitale sectoren. Immers, voor een adequate uitoefening van haar taken is het NCSC in grote mate afhankelijk van de informatie die zij van anderen over deze doelgroep ontvangt.[8] De minister stelt dan ook terecht dat dit punt op de lange termijn aandacht behoeft.[9]

**Vraag:** Hoe gaat de minister op de korte termijn actie ondernemen om ervoor zorgen dat de taken en verantwoordelijkheden van het NCSC en de NCTV door relevante partijen voldoende worden erkend?

**Vraag:** Hoe kan de minister op de korte termijn garanderen dat de communicatie en coördinatie tussen het NCSC en haar doelgroep wordt verbeterd, anders dan de herhaalde oproep aan haar doelgroep om het volledig en up-to-date houden van de bij het NCSC beschikbare informatie?

6 "Het NCSC is op het gebied van cyber security het centrale punt in Nederland en daarmee de spin in het web." Zie "Antwoord vragen van de leden Oosenbrug en Recourt over de reactie op een grote botnet-infectie door het Nationaal Cyber Security Centrum", TK 2012-2013, AH 2204, antwoord op vraag 6 en 7.
7 TK 2012-2013, 260643, nr. 272, p. 2 (Acties op korte termijn).
8 TK 2012-2013, 26 643, nr. 268, p. 3 (Acties in de aankomende periode).
9 TK 2012-2013, 260643, nr. 272, p. 3 (Acties met uitwerking op langere termijn).

## 4. Noodzaak extreme maatregelen niet aangetoond

*(a) Nationaal detectie- en responsenetwerk*

Naar aanleiding van Pobelka heeft de minister een aantal acties aangekondigd die ervoor moeten zorgen dat blijvend adequaat kan worden opgetreden tegen digitale dreigingen zoals botnets. Een van deze acties is het op- en uitbouwen van een Nationaal Detectie en Response Netwerk.[10] Wat dit precies zal inhouden is door de minister niet toegelicht, maar het vermoeden bestaat dat dit ziet op de analyse van elektronisch verkeer van de Rijksoverheid en de vitale sectoren door middel van Deep Packet Inspection (DPI). Met deze techniek wordt elektronisch dataverkeer tussen zender en ontvanger inhoudelijk geanalyseerd. Dit gaat om vertrouwelijke e-mails en chatberichten, maar bijvoorbeeld ook om zoekgedrag. Bovendien worden alle mensen die binnen de doelgroep van de Rijksoverheid en vitale sectoren werken maar óók iedereen waarmee zij communiceren door deze maatregel geraakt. De maatregel heeft dus grote gevolgen voor ons grondrecht op privacy en ons grondrecht op communicatievrijheid.

Zoals in de voorgaande paragrafen is geschetst, werd het inadequate overheidshandelen rondom Pobelka vooral veroorzaakt door een gebrek aan gevoel van urgentie, slechte samenwerking en gebrekkige informatie-uitwisseling tussen de verantwoordelijke partijen. In die omstandigheden, kan geen sprake zijn van een noodzaak tot nieuwe – inbreukmakende – bevoegdheden, zoals een nationaal detectie en responsenetwerk.[11] Zeker nu de noodzaak van deze actie ook elders niet door de minister is onderbouwd.

**Vraag:** Kan de minister het doel en de reikwijdte van de aangekondigde actie van het op- en uitbouwen van een Nationaal Detectie en Response Netwerk specificeren?

**Vraag:** Zal in de uitvoering van dit detectienetwerk gebruik worden gemaakt van DPI? Betekent dat dat de inhoud van alle dataverkeer van betrokkenen, dus bijvoorbeeld e-mails en chatberichten, wordt bekeken?

**Vraag:** Kan de minister de noodzaak voor een nationaal detectie en responsenetwerk feitelijk onderbouwen, daarbij rekening houdend met de mogelijke gevolgen van deze maatregel voor grondrecht op privacy en ons grondrecht op communicatievrijheid?

10 TK 2012-2013, 260643, nr. 272, p. 3 (Acties met uitwerking op langere termijn).
11 *Idem*.

*(b) Hackbevoegdheid*

Ook ontbreekt in het geheel enige noodzaak voor het zogenaamde 'hackvoorstel', dat de minister op 2 mei 2013 ter consultatie heeft voorgelegd.[12] Dit voorstel - dat tijdens het Algemeen Overleg Cybersecurity van 6 december 2012 uitvoerig is besproken - zou het voor de politie mogelijk maken om op afstand in te breken op de computer van burgers, software te installeren om hen te bespieden, rond te kijken en daar aanwezige gegevens te vernietigen. Dit zou moeten moeten bijdragen aan de opsporing en vervolging van computercriminaliteit, het bestrijding van botnets daarbij inbegrepen.[13] Het enkele "verstoren" van het kennisnemen van gegevens behoort daarbij tot de mogelijkheden.[14]

> **Vraag:** Uit welke omstandigheden, en het is duidelijk dat de Pobelka-casus daar niet toe behoort, blijkt de noodzaak, de proportionaliteit en de effectiviteit van de hackbevoegdheid als middel ter bestrijding van botnets?
>
> **Vraag:** Hoe zal de hackbevoegdheid als verstoringsmiddel worden vormgegeven? Is het een wens van de minister om deze bevoegdheid ook in te kunnen zetten bij digitale dreigingen zoals een DDoS-aanval? Zo ja, hoe ziet de minister dit dan voor zich nu de inzet van dit middel tot de opsporing en vervolging beperkt is?

Overigens zijn de vele vragen die uw Commissie de minister op 6 december 2012 over het hackvoorstel heeft gesteld, ondanks zijn uitdrukkelijke toezeggingen daartoe, in het wetsvoorstel en de toelichting daarop bijna geheel onbeantwoord gebleven. Mede met het oog op de lopende consultatie, is het belangrijk dat deze antwoorden alsnog worden afgedwongen. Het is daarom belangrijk om deze vragen opnieuw aan de minister voor te leggen. Een kopie van de brief met vragen die wij u ter voorbereiding van dat overleg hebben toegestuurd, vindt u in de bijlage.

Ik houd me graag beschikbaar voor overleg.

Met vriendelijke groet,

Simone Halink

12 Memorie van toelichting wetsvoorstel versterking aanpak computercriminaliteit, 2 mei 2013. Beschikbaar op: http://www.rijksoverheid.nl/ministeries/venj/documenten-en-publicaties/kamerstukken/2013/05/02/memorie-van-toelichting-wetsvoorstel-versterking-aanpak-computercriminaliteit.html.
13 *Idem*, p. 17.
14 *Idem*, p. 43.

BIJLAGE: Brief van Bits of Freedom aan de Commissie voor Veiligheid en Justitie over de bezwaren tegen het hackvoorstel, van 30 november 2012.