BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31(0)624534440
E axel.arnbak@bof.nl
W www.bof.nl

Bankrekening 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

Aan de leden van de Voortouwcommissie
Veiligheid en Justitie van de Tweede Kamer

Betreft:
Kamerbriefing Nationale Cybersecurity Strategie

Datum:
Amsterdam, 27 mei 2011.

Geachte dames en heren,

1. Op 1 juni 2011 vergadert de Voortouwcommissie Veiligheid en Justitie in het algemeen overleg Nationale Veiligheid over de Nationale Cybersecurity Strategie ('**NCSS**'). Dit overleg is de eerste gelegenheid dat de Tweede Kamer zich over dit nieuwe, complexe en belangrijke onderwerp buigt. Graag maakt de stichting Bits of Freedom ('**Bits of Freedom'**) gebruik van deze gelegenheid om u over cybersecurity en de NCSS te informeren.

2. **Bezint, eer ge begint**. De Tweede Kamer moet het beleidsterrein cybersecurity met dit adagium tegemoet treden. Bits of Freedom baseert dit op de volgende conclusies:

   - Er bestaat onvoldoende inzicht in de aard en omvang van de vraagstukken rondom cybersecurity;
   - Proportionaliteit als enige maatstaf voor nieuwe maatregelen leidt tot schending van het Europees Verdrag voor de Rechten van de Mens;
   - De nadruk op zelfregulering en publiek-private samenwerking vormt een gevaar voor de parlementaire democratie en onze internetvrijheid;
   - Een gebrek aan nuance over cybersecurity doet meer kwaad dan goed.

3. Op basis van deze analyse beveelt Bits of Freedom u aan om:

   - Een onafhankelijke, openbare en wetenschappelijke verantwoorde nulmeting naar de aard en omvang van aan cybersecurity gerelateerde vraagstukken te eisen;
   - Opvolging te geven aan de nulmeting via structurele, onafhankelijke en openbare rapportages;
   - De uitgangspunten van de NCSS in overeenstemming te brengen met de vereisten uit het Europees Verdrag voor de Rechten van de Mens en zijn vaste jurisprudentie;
   - Bij de regering af te dwingen dat zij de criteria uit de recente motie-Franken hanteert voor de toetsing van privacybeperkende maatregelen;
   - Terughoudend te zijn bij het steunen van zelfregulering en publiek-private samenwerking en parlementaire controle te eisen zodra grondrechten in het geding zijn;

4. Deze bevindingen worden hierna nader uitgewerkt.

Onvoldoende inzicht in aard en omvang vraagstukken rondom cybersecurity

5. In de NCSS wordt **aard** van de beleidsdoelen die met cybersecurity gemoeid zijn onvoldoende vastgesteld. In de NCSS is definitie van 'cybersecurity' dermate breed, dat vrijwel alles eronder verstaan kan worden.[1] Vervolgens schaart de NCSS de uiteenlopende verschijnselen i) weerbaarheid van vitale ict-infrastructuur (in §5.3), ii) strategische aanvallen op de nationale veiligheid (in §5.2) en iii) de opsporing van niet-strategische cybercriminaliteit (in §5.5) onder de noemer 'cybersecurity'.

6. Zo een brede focus is onwenselijk. De OECD concludeert in haar recente en gezaghebbende rapport 'Reducing Systemic Cybersecurity Risks' uit 2011 dat het op één hoop scharen van deze drie verschijnselen leidt tot 'grossly misleading conclusions'.[2] Zij verschillen namelijk sterk qua actoren, hun motieven en capaciteiten, doelwitten en hun kwetsbaarheid, aanvalsmethoden, duur, kans en impact. Het is goed mogelijk dat noch het garanderen van een weerbare vitale infrastructuur, noch de bescherming van de nationale veiligheid tegen aanvallen met grootschalige sociale- en economische impact, noch de bestrijding van niet-strategische (overwegend 'kleine') cybercriminaliteit[3] gebaat zijn bij de 'integrale aanpak' die de NCSS voorstaat. Deze hypothese dient onderwerp van de nulmeting te zijn, die Bits of Freedom cf. punt 8 adviseert.

7. In de NCSS wordt evenmin inzicht gegeven in de **omvang** van de problematiek rondom cybersecurity. De NCSS baseert zich op drie anekdotische voorvallen.[4] Buiten het feit dat deze voorvallen serieuze implicaties kunnen hebben, geeft noch de NCSS, noch het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 ('**Trendrapport**'),[5] noch de Verkenning cybercrime in Nederland 2009 ('**Verkenning**')[6] een helder overzicht van de omvang. Zij lijkt daarentegen op alle door de NCSS genoemde deelterreinen mee te vallen, met volgens de OECD als voornaamste oorzaak de decentrale opzet van het internet.[7]

> **Vitale infrastructuur:** het Trendrapport stelt onomwonden vast: 'overigens hebben zich tot dusverre geen publiekelijk bekend geworden incidenten voorgedaan in Nederland'.[8] **Nationale veiligheid**: Het Trendrapport stelt: 'er [is] weinig betrouwbare kwantitatieve data beschikbaar (...). Het gebrek aan kwantitatieve data belemmert niet alleen het inzicht in de trends zelf, maar ook het meten van het effect van maatregelen.'[9] Desalniettemin verwijzen zowel de NCTb als het Ministerie

1 'Cyber security is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.' NCSS, p.3.
2 P. Sommer and I. Brown, “Reducing Systemic Cybersecurity Risks”, OECD/IFP Project on 'Future Global Shocks', 14 jan. 2011, p.5/6. Zie: http://www.oecd.org/dataoecd/57/44/46889922.pdf
3 E.R. Leukfeldt, M.M.L. Domenie, W.Ph. Stol, 'Verkenning cybercrime in Nederland 2009', Den Haag: Boom Juridische Uitgevers 2010. Publicatiedatum: mei 2010, p.xxii
4 De Stuxnet-worm, het Bredolab-botnet en DDoS-aanvallen in reactie op genomen maatregelen tegen klokkenluiders-website Wikileaks. NCSS, p.2/3.
5 Rijksoverheid, 'Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010', Publicatiedatum: nov. 2010. In te zien via: http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/trendrapporten/trendrapport-2010.html.
6 E.R. Leukfeldt, M.M.L. Domenie, W.Ph. Stol, 'Verkenning cybercrime in Nederland 2009', Den Haag: Boom Juridische Uitgevers 2010. Publicatiedatum: mei 2010. Niet online beschikbaar.
7 Door de decentrale opzet van het internet wordt informatie omgeleid via een andere routes als een belangrijke node uit het netwerk, zoals de Amsterdam Internet Exchange, wegvalt. De OECD noemt op basis van vele case-studies ook de snelle responscapaciteit bij eerdere cyberaanvallen als belangrijke oorzaak. P. Sommer and I. Brown, “Reducing Systemic Cybersecurity Risks”, OECD, p.80/81.
8 Trendrapport, §3.2, p.20. Een vaststelling gemaakt in het kader van Nederlandse procescontrolesystemen, of Industrial Control Systems (ICS).
9 Trendrapport, §7.5, p.45.

van Defenisie naar het Trendrapport voor de onderbouwing van hun beleid.[10] De OECD komt tot de conclusie dat 'cyber attacks are unlikely to cause problems [for national security]. Instead, trouble caused by cyber attacks is likely to be localised and short-lived.' De gerenommeerde onderzoekers – van de London School of Economics en de universiteit van Oxford – achten 'a pure cyberwar, that is one fought solely with cyber-weapons, unlikely.'[11] **Cybercriminaliteit:** in de Verkenning vonden onderzoekers in 665 onderzochte dossiers geen aanwijzingen voor georganiseerde cybercriminaliteit. Zij concludeerden dat “er veel 'kleine delicten' gepleegd worden door min of meer alledaagse verdachten die individueel opereren”.[12] Verder stelt de Verkenning vast dat er 'weinig bekend is over de omvang van cybercrime'.[13] Een ander rapport, van de KLPD, spreekt over een 'exponentiële groei' van high tech crime,[14] maar ontnuchterende cijfers van het CBS laten zien dat deze vorm van criminaliteit in Nederland weinig voorkomt: in 2008 zijn 901 misdrijven geregistreerd.[15] De Verkenning noemt dit getal 'erg laag' en spreekt het vermoeden van een lage aangiftebereidheid uit.[16] Maar ook al zou deze bereidheid hoger zijn, blijft het aantal misdrijven zeer laag. Tegelijkertijd dient bedacht te worden, dat de afgelopen jaren een forse stijging hebben laten zien in zowel gebruik van breedband als mobiel internet. Een stijging van cybercriminaliteit is daaraan inherent. Het is belangrijk om in een vroeg stadium deze vorm van criminaliteit aan te pakken, maar waakzaamheid blijft geboden tegen het overdrijven van de problematiek.

8. **Advies aan de Tweede Kamer**: **eis een onafhankelijke, openbare en wetenschappelijk verantwoorde nulmeting naar de aard en omvang van aan cybersecurity gerelateerde vraagstukken**. **Laat vervolgens via structurele, onafhankelijke en openbare rapportages opvolging aan de nulmeting geven**. Structureel inzicht in de aard en de omvang van de vraagstukken rondom cybersecurity is nodig om tot gedegen beleid te komen op dit nieuwe, complexe en belangrijke onderwerp. Uit bestaande rapportages lijkt de problematiek eerder mee te vallen. Een onderdeel van de nulmeting is de afweging of de bestrijding van niet-strategische cybercriminaliteit onderdeel dient te zijn van de NCSS.

'Proportionaliteit' als enige maatstaf voor nieuwe maatregelen leidt tot schending van het Europees Verdrag voor de Rechten van de Mens

9. Het is evident dat maatregelen die worden genomen in het kader van cybersecurity een negatieve impact op fundamentele rechten kunnen hebben. De NCSS schrijft dan ook dat digitale grondrechten ‘overeind dienen te blijven’.[17] Dit prijzenswaardige uitgangspunt is in overeenstemming met de in het regeerakkoord opgenomen ambitie een 'vrij en open internet' te bevorderen.

10. Maar de nadere invulling in de NCSS van dit uitgangspunt – ‘te nemen maatregelen zijn proportioneel’[18] – blijft achter bij de vereisten van het Europees Verdrag voor de Rechten van de Mens (‘**EVRM**'). Het EVRM staat beperkingen van digitale grondrechten pas toe indien zij 'noodzakelijk in een democratische samenleving' en 'bij wet voorzien' zijn. Bovendien moet de wezenlijke kern van digitale grondrechten niet aangetast worden.

11. Het criterium '**noodzakelijk in een democratische samenleving**' omvat meer dan

10 In een recent interview met weekblad *Vrij Nederland,* verwijzen Nationaal Coördinator Terrorismebestrijding Erik Akerboom en Generaal-Majoor Koen Gijsbers, coördinator van de Nederlandse cyberactiviteiten op het Ministerie van Defensie, herhaaldelijk naar het Trendrapport als basis voor hun activiteiten. Bron: M. Martijn en F. Vuijst, 'De virtuele oorlog', Vrij Nederland, 28 mei 2011, p. 31. Niet online beschikbaar.
11 Trendrapport, §7.5, p.45.
12 Verkenning, p.xxii
13 Verkenning, p.xxiv.
14 KLPD, 'Overall-beeld Aandachtsgebieden', 14 jul. 2010, p.21, te vinden via: https://www.bof.nl/live/wp-content/uploads/Rapport-Nationale-Recherche-KLPD-Overall-beeld-Aandachtsgebieden.pdf
15 CBS Statline, via deze link te raadplegen. Zie voor meer informatie het commentaar van Bits of Freedom via: https://www.bof.nl/2010/08/23/politierapport-over-high-tech-crime-ongenuanceerd/
16 Verkenning, p.xxiv.
17 NCSS, p.4.
18 Idem.

proportionaliteit alleen. Wil aan het criterium van ‘noodzaak’ voldaan zijn, dan dient i) een dringende maatschappelijke behoefte vast te staan en moet de maatregel ii) proportioneel zijn, oftewel dienen maatregelen in verhouding te staan tot hun doel. Daarbij dient gekeken te worden naar de effectiviteit, subsidiariteit – of er ook alternatieven bestaan die minder schadelijk zijn voor grondrechten en tot hetzelfde resultaat leiden – en beperkingen van de inbreuk (bijvoorbeeld: slechts na machtiging rechter-commissaris).[19]

> In het leerstuk van de ‘pressing social need’, de dringende maatschappelijke behoefte, geldt dat ‘noodzakelijk’ geen synoniem van ‘nodig’ is, en niet de flexibiliteit van woorden als ‘nuttig’ of ‘wenselijk’ heeft. Het Europees hof voor de Rechten van de Mens past daarmee een zware toets toe bij het toelaten van inperkingen. Om aan het proportionaliteitsvereiste te voldoen, dient een belangenafweging plaats te vinden tussen het nastreven van dit legitieme belang en de impact die dit heeft op het grondrecht. Daarbij geldt dat de lat hoger komt te liggen naarmate de inbreuk op het grondrecht ernstiger is.[20]

12. Het sub-criterium *dringende maatschappelijke behoefte* is hier van bijzondere betekenis. Er bestaat immers onvoldoende inzicht in de omvang van de problematiek rondom cybersecurity (cf. punt 7). Het uitgangspunt van de NCSS dat grondrechten 'overeind dienen te blijven' maakt het treffen van maatregelen op het gebied van cybersecurity die de grondrechten beperken niet mogelijk. De dringende maatschappelijke behoefte is immers onvoldoende aangetoond (de problematiek lijkt eerder mee te vallen, cf. punt 7).

13. Het criterium '**bij wet voorzien**' is vergelijkbaar met het Nederlandse legaliteitsbeginsel. Dit criterium verzekert dat beperkingen van grondrechten een wettelijke basis kennen en niet zonder instemming van het parlement worden getroffen. Het is van cruciaal belang dat dit criterium wordt meegenomen in de NCSS, omdat de strategie sterk inzet op zelfregulering en publiek-private samenwerking. Na punt 18 wordt verder ingegaan op de gevaren van deze nadruk op publiek-private samenwerking op de parlementaire democratie en onze internetvrijheid.

> De voorwaarde dat een inperking 'bij wet voorzien' moet zijn, valt in drie deelcriteria uiteen. Ten eerste moet de maatregel in nationale wetgeving zijn vastgelegd. Een Algemene Maatregel van Bestuur (AmvB) valt hier ook onder. De maatregelen dienen tevens voldoende ‘toegankelijk voor het publiek’ te zijn (via publicatie in de Staatscourant, bijvoorbeeld). Ten derde moet er sprake zijn van ‘foreseeability’, de inbreuk moet voorzienbaar zijn. Dit houdt in dat er voldoende waarborgen worden getroffen tegen willekeur en misbruik door de bevoegde autoriteiten en dat burgers de effecten van een maatregel moeten kunnen inschatten.[21] Als praktische handvatten hanteert het Europees Hof voor de Rechten van de Mens drie leidende beginselen, te weten transparantie, effectieve notificatie en het zwaarder worden van het foreseeability-vereiste naarmate de inbreuk op het EVRM toeneemt.[22] Zo dient de bevoegdheid om een internettap te plaatsen transparant toegepast te worden gezien de hevigheid van deze inbreuk.[23]

14. Volgens vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens is de **wezenlijke kern van grondrechten onaantastbaar.**[24] Het 'Rapport Staatscommissie Grondwet' vult dit criterium als volgt in: 'zelfs als een beperking van een grondrecht het enige middel is om een bepaald doel te bereiken, en zelfs als dit doel van zwaarwegend belang is, is zo'n beperking niet aanvaardbaar voor zover zij de kern van het grondrecht aantast.'[25] Draconische maatregelen, zoals het aftapbaar maken van het gehele internet bij internetknooppunten met behulp van de technologie *deep packet inspection,* zijn daarmee

19 EHRM 25 maart 1983, nr. 5947/72, Silver a.o. v. The United Kingdom, nr. 97.
20 Idem.
21 EHRM 1 juli 2008, nr. 58243/00, Liberty a.o. v. The United Kingdom, par. 62.
22 EHRM 25 maart 1983, nr. 5947/72, Silver a.o. v. The United Kingdom, par. 48.
23 Over het afluisteren van telefonie oordeelde het Hof: “procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge”. EHRM 1 juli 2008, appl. 58243/00, Liberty a.o. v. The United Kingdom, par. 67.
24 EHRM 11 juli 2002, nr. 28957/95, Goodwin v The United Kingdom. Geciteerd uit Rapport Staatscommissie Grondwet, p.56.
25 Rapport Staatscommissie Grondwet, 21 nov. 2011, p.56, in te zien via:
http://www.staatscommissiegrondwet.nl/userfiles/files/Rapport%20Staatscommissie%20Grondwet_lowres(1).pdf

illegaal. Zij tasten het grondrecht op privacy in de kern aan – na een wholesale internettap blijft er niets meer van over.

15. **Advies aan de Tweede Kamer**: **breng de uitgangspunten van de NCSS in overeenstemming met de vereisten uit het Europees Verdrag voor de Rechten van de Mens en zijn vaste jurisprudentie.** De criteria 'noodzakelijk in een democratische samenleving', 'bij wet voorzien' en 'wezenlijke kern van grondrechten onaantastbaar' dienen in de NCSS opgenomen te worden om invulling te geven aan het uitgangspunt dat 'grondrechten overeind dienen te blijven'.[26]

16. Op het specifiekere gebied van privacy wijst Bits of Freedom u graag op de recent in grote meerderheid aangenomen **motie-Franken (CDA) over de toetsing van privacybeperkende maatregelen**.[27] De motie zet een vijftal criteria uiteen waaraan nieuwe privacybeperkende maatregelen voorafgaand aan hun introductie getoetst moeten worden. De regering dient tevens verslag te doen van deze toetsing in de Memorie van Toelichting. De vijf criteria en de rapportage in de Memorie van Toelichting garanderen een gedegen besluitvorming op dit nieuwe en complexe onderwerp en geven het parlement direct inzicht in de beweegredenen van de regering om te pleiten voor het inperken van de privacy van Nederlanders.

> De vijf criteria uit motie-Franken:
> I. De noodzaak, effectiviteit en hanteerbaarheid van de maatregel;
> II. De proportionaliteit: de inbreuk mag niet groter zijn dan strikt noodzakelijk is;
> III. De resultaten van een Privacy Impact Assessment, zodat vooraf is onderzocht welke risico's de maatregel met zich meebrengt;
> IV. De mogelijkheid van een effectief toezicht en controle op de uitvoering van de maatregel, te realiseren door onder meer audits door de onafhankelijke toezichthouder;
> V. Beperking van de geldigheidsduur door een horizonbepaling of in ieder geval een evaluatiebepaling.

17. **Advies aan de Tweede Kamer**: **dwing bij de regering af dat zij de criteria uit de recente motie-Franken hanteert voor de toetsing van privacybeperkende maatregelen.** De vijf criteria en de rapportage in de Memorie van Toelichting garanderen een gedegen besluitvorming op dit nieuwe en complexe onderwerp en geven het parlement direct inzicht in de beweegredenen van de regering.

De nadruk op zelfregulering en publiek-private samenwerking vormt een gevaar voor de parlementaire democratie en internetvrijheid

18. De NCSS kent een sterke nadruk op publiek-private samenwerking en zelfregulering, die zelfs wordt weerspiegeld in de ondertitel van de strategie ('slagkracht door samenwerking'). Dit sluit aan bij een trend op het gebied van internetregulering, waarin overheden en het bedrijfsleven steeds intensiever samenwerken. De nadruk in de NCSS op deze samenwerking vormt een gevaar voor de parlementaire democratie en internetvrijheid.

> In een recente studie beschrijft European Digital Rights ('EDRi'), de Europese koepelorganisatie van Bits of Freedom, hoe overheden in geheel Europa – ook in Nederland – internetregulering steeds vaker uitbesteden aan private partijen.[28] Voor beide partijen is dit interessant. Via het bedrijfsleven kan de overheid verdergaande maatregelen voorstellen, omdat publiek-private

26 NCSS, p.4.
27 *Kamerstukken I*, 2011, 31 051, nr. D, Motie-Franken (CDA) c.s. over criteria in het geval van nieuwe wetsvoorstellen waarbij van een beperking op het grondrecht van de bescherming van de persoonlijke levenssfeer sprake is, zie: http://www.eerstekamer.nl/motie/motie_franken_cda_c_s_over. NB: alleen de VVD-fractie stemde tegen.
28 J. McNamee, *'The Slide from "Self-regulation" to Corporate Censorship'*, European Digital Rights, Jan. 2011. Zie: http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf

samenwerkingen en zelfreguleringsinitiatieven niet zijn onderworpen aan parlementaire controle. Bedrijven zijn daarnaast minder gebonden aan rechtstatelijke vereisten, zoals algemene maatregelen van behoorlijk bestuur uit de Algemene wet bestuursrecht (transparantiebeginsel, zorgvuldigheidsbeginsel, legitimiteitsbeginsel, etc.). Ook vanuit financieel oogpunt is publiek-private samenwerking aantrekkelijk. Internetregulering belandt zo op de balans van het bedrijfsleven en komt niet of in mindere mate ten laste van de staatskas. Ondanks deze financiële gevolgen, kent ook het bedrijfsleven sterke prikkels om publiek-private samenwerking te ondersteunen. Via deze weg kan de invloed op internetregulering én de zeggenschap over netwerken, diensten en eindgebruikers vergroot worden. Bits of Freedom zal in de komende maanden structureel aandacht besteden aan deze trend, die zij de 'privatisering van controle' noemt.

19. De **parlementaire democratie** gaat uit van *checks and balances*: een gekozen volksvertegenwoordiging toetst en controleert overheidsbeleid. Initiatieven die voortkomen uit publiek-private samenwerking volgen echter niet de gangbare route langs parlementaire controle. Met de sterke nadruk in de NCSS op publiek-private samenwerking en zelfregulering ('zelfregulering als het kan, wetgeving als het moet'),[29] riskeert het parlement de democratische controle te verliezen op dit beleidsterrein, terwijl cybersecurity iedere Nederlander raakt. Het parlement dient daarom zeer terughoudend te zijn bij het steunen van publiek-private samenwerking en steeds volledige inzage te eisen in de voortgang op het cybersecurity-dossier.

De ontstaansgeschiedenis en recente afschaffing van internetfiltering van afbeeldingen met seksueel kindermisbruik illustreert het probleem van publiek-private samenwerking in verband met het omzeilen van parlementaire controle. Rond 2004 zijn de eerste stappen gezet voor een systeem van internetfiltering, waarbij de overheid een zwarte lijst zou aanleveren aan providers om websites te kunnen blokkeren. Nadat de Vrij Universiteit e.a. had geconcludeerd dat de lijst werd aangeleverd door de KLPD en dat deze maatregel niet 'bij wet voorzien' was (cf. punt 13 van deze Kamerbrief),[30] werd vastgesteld dat zo een publiek-private samenwerking voor internetfiltering in strijd is met onze Grondwet. Vervolgens besloot het ministerie van Justitie het Meldpunt Kinderporno op te laten richten door de providers, een private instelling die de zwarte lijst met te blokkeren websites zou aanleveren. Met deze opgelegde vorm van 'zelfregulering' verdwenen de internetfilters van de radar van het parlement en werd het voor burgers onmogelijk om met een beroep op de Wet openbaarheid van bestuur in kennis gesteld te worden van de voortgang.[31] Pas in mei 2011, tijdens het voortgangsoverleg aanpak seksueel kindermisbruik, heeft de Tweede Kamer op basis van nieuwe informatie van de huidige minister van Veiligheid en Justitie en na de nodige media-aandacht over dit vraagstuk, parlementaire controle kunnen uitvoeren en haar steun ingetrokken voor deze ineffectieve en schadelijke internetfilters.[32] Ruim zeven jaar lang heeft het ministerie de Tweede Kamer getracht te omzeilen, is het parlement onterecht in de veronderstelling gelaten dat de ernstige problematiek met filters kon worden aangepakt en is het parlement onvoldoende geïnformeerd door het ministerie.[33]

20. De **internetvrijheid van eindgebruikers** kan slechts beperkt worden als aan strikte vereisten van het EVRM is voldaan (cf. punt 9-17 van deze Kamerbrief). Een belangrijk kenmerk van publiek-private samenwerking, is dat de maatregelen die hieruit voortkomen vaak buiten het zicht van het parlement en de samenleving worden ingevoerd (niet 'bij wet voorzien') en verder gaan dan de grondwettelijke criteria toelaten (niet 'noodzakelijk in een democratische samenleving').

Ook met betrekking tot internetvrijheid illustreert de ontstaansgeschiedenis en recente afschaffing van internetfiltering van afbeeldingen met seksueel kindermisbruik het probleem van publiek-private samenwerking en zelfregulering. Van meet af aan is het evident dat internetfiltering op initiatief van de overheid in strijd is met artikel 7 van de Grondwet, dat een verbod op preventieve censuur inhoudt (niet 'noodzakelijk in een democratische samenleving'). Daarna werd het Platform Internetveiligheid opgericht, waarin bedrijven zouden samenwerken om internetfilters op te leggen

29 NCSS, p.3/4.
30 Stol, W. Ph., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R., Lodder, A.R., *'Filteren van kinderporno op internet',* Vrije Universiteit, WODC e.a., Den Haag: Boom Juridische Uitgevers 2008, p.iv, te raadplegen via: https://www.wodc.nl/images/1616_volledige_tekst_tcm44-117157.pdf
31 Bits of Freedom, *'Geen openheid over maatregelen tegen buitenlandse misbruiksites'*, 12 nov. 2010, op basis van kamervragen van de VVD-fractie, zie: https://www.bof.nl/2010/10/12/geen-openheid-over-maatregelen-tegen-buitenlandse-misbruiksites/
32 NU.nl, *'Politiek blokkeert internetfilter'*, 18 mei 2011, zie: http://www.nu.nl/internet/2517775/politiek-blokkeert-internetfilter.html. Voor commentaar Bits of Freedom, zie: https://www.bof.nl/2011/05/20/internetfilter-kamer-kiest-voor-belang-kind-tegen-censuur/
33 BBC News, *'Risk of Cyberwar over-hyped, says OECD report'*, 17 jan. 2011, zie: http://www.bbc.co.uk/news/mobile/technology-12205169; CNN News, *'Schneier: Threat of "Cyberwar" Has Been Hugely Hyped'*, 7 jul. 2010, te vinden via: http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/

aan internetgebruikers (niet 'bij wet voorzien').[34] Uiteindelijke steunt de Tweede Kamer de filters niet langer.[35] Maar ruim zeven jaar lang heeft het erom gespannen of deze evidente schending van de internetvrijheid van eindgebruikers via de private route zou worden ingesteld. De studie van EDRi bevat twaalf andere concrete voorbeelden van deze tendens.[36]

21. De Tweede Kamer dient echter ten volle haar parlementaire controle uit te voeren wanneer de internetvrijheid in het geding is, in het bijzonder wanneer maatregelen via publiek-private samenwerking tot stand komen. Dit geldt voor de eigen parlementaire behandeling en voor die in de Eerste Kamer. De Senaat komt pas aan haar rechtstatelijke verantwoordelijkheid – toetsing van de verenigbaarheid van beleid aan de Grondwet en internationale verdragen – toe, als de Tweede Kamer parlementaire controle opeist.

22. **Advies aan de Tweede Kamer**: **terughoudend te zijn bij het steunen van publiek-private samenwerking en zelfregulering en parlementaire controle te eisen zodra grondrechten in het geding zijn**. De intensieve samenwerking tussen overheid en bedrijfsleven heeft namelijk een negatieve uitwerking op de parlementaire democratie en internetvrijheid.

Gebrek aan nuance over cybersecurity doet meer kwaad dan goed

23. Bits of Freedom constateert tenslotte een **gebrek aan nuance** in vele debatten en publicaties over het nieuwe en complexe fenomeen cybersecurity. De OECD stelt ook vast dat 'unfortunately too many published assessments have favoured sensationalism over careful analysis'.[37] Wereldwijd erkende experts op het gebied van cybersecurity spreken van een 'hype'.[38]

24. De OECD roept op tot 'discipline in the use of language'. Een gebrek aan nuance zal namelijk gepaard gaan met een verkeerde focus, het niet aanpakken van daadwerkelijke problemen, onjuiste allocatie van financiële middelen en verspilde tijd. Daarvoor zijn het garanderen van een betrouwbare en weerbare ict-infrastructuur, onze nationale veiligheid, de bestrijding van cybercriminaliteit én het beschermen van internetvrijheid te belangrijke onderwerpen. Bits of Freedom vertrouwt erop dat u de oproep tot nuance ter harte neemt.

Over Bits of Freedom

Bits of Freedom verdedigt de internetvrijheid en privacy van Nederlandse internetgebruikers. Zij doet dat door constructieve campagnes te voeren en de overheid te informeren. Uiteraard houdt Bits of zich graag beschikbaar voor een nadere toelichting.

Hoogachtend,

Axel Arnbak

---

34 Website Platform Internetveiligheid, onder publiek-privaat initiatief van ECP-EPN, zie: http://www.ecp-epn.nl/platform-internetveiligheid
35 NU.nl, *'Politiek blokkeert internetfilter'*, 18 mei 2011, zie: http://www.nu.nl/internet/2517775/politiek-blokkeert-internetfilter.html. Voor commentaar Bits of Freedom, zie: https://www.bof.nl/2011/05/20/internetfilter-kamer-kiest-voor-belang-kind-tegen-censuur/
36 J. McNamee, *'The Slide from "Self-regulation" to Corporate Censorship'*, European Digital Rights, Jan. 2011. Zie: http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf
37 OECD, p.80.
38 BBC News, *'Risk of Cyberwar over-hyped, says OECD report'*, 17 jan. 2011, zie: http://www.bbc.co.uk/news/mobile/technology-12205169. CNN News, *'Schneier: Threat of "Cyberwar" Has Been Hugely Hyped'*, 7 jul. 2010, te vinden via: http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/