Dit voorstel leidt tot een disproportionele inperking van de privacy. Het heeft onaanvaardbare gevolgen heeft voor de internetvrijheid en veiligheid van (Nederlandse) internetters en leidt tot een schending de soevereiniteit van andere landen door Nederland.
De tegenreactie die dit uitlokt heeft alarmerende gevolgen voor de soevereiniteit van Nederland en voor cybersecurity en mensenrechten wereldwijd.

Volgens de minister zijn deze bevoegdheden nodig om cybercrime te bestrijden. Onderbouwing van enige noodzaak daartoe en van de proportionaliteit en effectiviteit van de voorgestelde bevoegdheden schiet echter ernstig tekort. De minister laat verder weten dat – ondanks dat de bevoegdheid daartoe blijkbaar ontbrak – de politie het afgelopen jaar al inbrak in computers, die computers doorzocht en zelfs gegevens heeft vernietigd op servers in het buitenland.

De minister schrijft dat "een inhaalslag nodig is om de opsporing en vervolging van cybercrime te versterken". Vervolgens schetst de minister weliswaar een aantal problemen bij de opsporing, zoals de achterblijvende "kennis en ervaring binnen de strafrechtketen" en technische innovatie die handig wordt gebruikt door criminelen, maar hoe de voorgestelde maatregelen die problemen specifiek gaan oplossen en of ze noodzakelijk, proportioneel en effectief zijn, wordt niet onderbouwd. Het mag duidelijk zijn dat deze flinterdunne onderbouwing voor een wetsvoorstel onacceptabel is, zeker als het om zo een verstrekkend voorstel gaat.
Daarnaast zijn de bevoegdheden van de minister gericht op het bestrijden van strafbare feite nadat deze hebben plaatsgevonden. In cybersecurity is het echter zeer gebruikelijk om in plaats daarvan maatregelen te nemen om te zorgen dat bepaalde inbreuken niet plaatsvinden door het nemen van preventieve maatregelen, zoals het vergroten van de expertise en capaciteit op het gebied van cybersecurity. Het is opvallend dat de minister daaraan geen aandacht besteed.

Het voorstel van de minister leidt tot een ernstige inperking van de privacy, niet alleen van de verdachte maar ook van onschuldige Nederlanders. Zo hebben de voorgestelde bevoegdheden veel grotere gevolgen voor de privacy van betrokkenen. Bij het aftappen van telefoongesprekken of het plaatsen van afluisterapparatuur geldt al dat niet alleen de verdachte wordt afgeluisterd maar ook al die personen waarmee de verdachte via die lijn of in die woning communiceert. De privacy-implicaties van het doorzoeken van computers zijn echter nog eens tien keer groter: alle mailtjes, alle foto’s en alle berichten op sociale media die een verdachte met onschuldige Nederlanders heeft uitgewisseld, komen in het vizier van de opsporing.
Het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden vereist dat maatregelen die fundamentele rechten – zoals het recht op privacy – beperken, noodzakelijk in een democratische samenleving en proportioneel zijn. Dit moet voorafgaand aan de invoering van die maatregelen zijn aangetoond, zoals ook blijkt uit de motie Franken. De minister schetst weliswaar een aantal problemen die moeilijk zijn voor opsporing, maar hoe de voorgestelde maatregelen die problemen specifiek gaan oplossen en of ze noodzakelijk, proportioneel en effectief zijn, wordt niet onderbouwd. Daarmee is het voorstel in strijd met voornoemd verdrag.

Als de politie bij computers moet kunnen inbreken, heeft ze er belang bij dat die systemen kwetsbaar blijven. De politie kan immers slechts inbreken bij systemen die onvoldoende beveiligd zijn. Dit geeft de overheid een perverse prikkel om informatie over kwetsbaarheden voor zichzelf te houden in plaats van deze te delen met Nederlandse internetgebruikers. Die kunnen hun eigen informatiesystemen daardoor minder goed beschermen. Dit staat lijnrecht tegenover alle investeringen van de overheid in cybersecurity over de afgelopen jaren.

Bovendien geldt dat spyware moeilijk binnen de perken te houden is. In

Duitsland hebben ze dat al ervaren. Uit onderzoek van de hackersvereniging Chaos Computer Club bleek dat heimelijk door de politie geïnstalleerde afluistersoftware makkelijk te hacken was – via het internet. 3
Zodat niet alleen
de politie een computer kon overnemen met behulp van spyware, maar dat ook criminelen diezelfde computer konden overnemen, omdat de spyware zélf gehackt was. De politie maakt zich in dat geval ook nog eens kwetsbaar voor computerinbraken via diezelfde software.
Verder bestaat het risico dat ingezette spyware zich verder verspreidt en onschuldige systemen infecteert; dit gebeurde onder meer bij het virus Stuxnet dat was ontwikkeld voor kernreactoren in Iran, maar ook systemen in de Verenigde Staten geïnfecteerd blijkt te hebben.

Bovendien leiden de voorgestelde bevoegdheden tot veel praktische problemen. Hoe zal de overheid bijvoorbeeld omgaan met antivirussoftware? Immers, als antivirussoftware de spyware van de Nederlandse politie op een computer aantreft, zou dat in principe aan de gebruiker moeten worden gemeld. De vraag is dus of de overheid van antivirusbedrijven zal verwachten of hen ertoe zal verplichten dat ze overheids-spyware niet detecteren, melden of verwijderen, met het gevolg dat gebruikers extra kwetsbaar zijn. Over dit probleem heeft Kamerlid Berndsen-Jansen (D66) de minister op 14 november 2012 reeds kritische vragen gesteld.

Een ander praktisch probleem is dat de bevoegdheden erg makkelijk misbruikt kunnen worden. Juist doordat deze opsporingshandelingen digitaal zijn is het moeilijk na te gaan of bewijs is gefabriceerd of juist is achtergehouden. Een hieraan gerelateerd voorbeeld: in Duitsland is gebleken dat de spyware die bedoeld was om alleen Skype gesprekken af te luisteren, in de praktijk ook ingezet kon worden voor het op afstand aanzetten van de camera. In Duitsland trokken onderzoekers dan ook de conclusie dat deze software niet geschikt was voor bewijsvergaring.

De internationale gemeenschap maakt zich ernstig zorgen over de hiervoor genoemde punten, zoals blijkt uit bijgaande brief. Meer dan 40 organisaties die zich inzetten voor digitale burgerrechten hebben deze brief ondertekend. Gezien de grote risico's die het voorstel heeft voor cybersecurity en de bescherming van mensenrechten wereldwijd, roept een brede internationale coalitie van maatschappelijke organisaties de minister in die brief op om zijn voorstel in te trekken.