Stichting Digitale
Infrastructuur Nederland

Position paper DINL

t.b.v. hoorzitting/rondetafelgesprek Wet op de inlichtingen- en veiligheidsdiensten
d.d. 15 december 2016

Stichting Digitale Infrastructuur Nederland (DINL) is de koepelorganisatie en spreekbuis van de Nederlandse aanbieders van digitale infrastructuur. Die sector vormt de basis van Nederlands digitale mainport. Nederland heeft dankzij die mainport een sterke positie verworven als vestigingsplaats voor aanbieders van online diensten. Grote Internet merken als Google, Facebook, Netflix, Uber, Akamai openden datacenters en kantoren in Nederland en zorgen voor nieuwe economische activiteit en werkgelegenheid. Het CBS becijfert dat thans 50.000 bedrijven en 335.000 werknemers hun geld verdienen met online activiteiten.

Kernwaarden
Die online economie kon ontstaan door het vertrouwen van burgers en bedrijven in de vrijheid, openheid en veiligheid van het Internet. Daarmee kunnen ze internationaal ondernemen, zonder beperkingen communiceren, hun mening uiten, gegevens opslaan bij online dienstverleners in binnen- en buitenland. Het uitdragen van het belang van de vrijheid, openheid en veiligheid van het Internet is daarom niet voor niets kabinetsbeleid, het is herkend als een essentiële randvoorwaarde voor vertrouwen in de Nederlandse Internet economie.

Aanbeveling commissie Dessens
DINL kan zich in principe vinden in de analyse van de commissie Dessens: een modernisering van de huidige wet op de inlichtingen- en veiligheidsdiensten is wenselijk. Er moet in die wet dan wel een nieuwe balans worden gevonden tussen economische belangen en bescherming van de kernwaarden enerzijds, en de mogelijkheden voor handhaving en opsporing anderzijds. Maar die balans is in het huidige wetsvoorstel verstoord.

Van risico naar Kans
DINL is van mening dat met enkele essentiële wijzigingen de balans kan worden hersteld. Daarmee verandert de wet van een risico, in een kans voor Nederland! Met een goede borging van de kernwaarden en met verbeterd toezicht, wordt Nederland een land waar ingrijpende bevoegdheden niet zomaar worden ingezet voor het verzwakken van veiligheid. En waar de rechten van burgers en bedrijven voldoende worden beschermd. Dat werkt vertrouwen en versterkt daarmee de economische positie van ons land.

Uitvoering treft aanbieders van digitale infrastructuur
Door de manier waarop de bevoegdheden van de diensten in het voorliggende wetsvoorstel WIV worden uitgewerkt, worden systemen en netwerken van aanbieders van digitale infrastructuur bij ingrepen van de diensten, verzwakt voor alle gebruikers. DINL schetst de knelpunten die raken aan openheid, vrijheid en veiligheid van het Internet en hun diensten.

Toezicht
Wetenschap (Ivir), de Raad van State en de Raad voor de Rechtspraak komen allen tot de conclusie dat het huidige en voorgestelde toezicht ontoereikend is. DINL is van mening dat goed toezicht essentieel is voor het vertrouwen. Het moet zodanig worden ingericht dat het juridische toetsing kan doorstaan. Zodat burgers en bedrijven er op kunnen rekenen dat hun

Stichting Digitale Infrastructuur Nederland
Overgoo 13 / Postbus 262
2260 AG Leidschendam

T: +31707621070
E: info@dinl.nl

belangen ook bij het handelen van de inlichtingendiensten voldoende worden beschermd. DINL sluit zich daarom aan bij de zienswijze van het Ivir (Instituut voor ICT en Recht) , dat een gedegen toezichtsregime beschrijft in haar document “10 standards for oversight” .

Kernwaarde: Veilig
Het uitgangspunt in de beleidsafwegingen behoort te zijn dat de beveiliging van netwerken, systemen en data altijd een hogere prioriteit heeft dan het opsporingsbelang. Het compromitteren van veiligheidssystemen, of verzwakken daarvan om inlichtingen of opsporing mogelijk te maken, is wat DINL betreft ontoelaatbaar. Het kabinet maakt in haar standpunt op het gebied van versleuteling (januari 2016) terecht die belangenafweging: de beveiliging van informatie heeft een hogere prioriteit dan het opsporingsbelang. Dat principe moet daarom ook leidend zijn voor alle andere beveiliging. In concreto:

- Wegnemen van perverse prikkels: geen handelen (aankopen) van kwetsbaarheden, of andere activiteiten die de handel in zero day kwetsbaarheden stimuleren.
- Geen gebruik maken van structurele zwakheden zonder dat deze onverwijld gemeld worden aan bedrijven.
- Geen structurele inbreuken op generieke versleutelingssystemen (TTP, certificaten, SSL) en andere veiligheidssystemen.

Kernwaarde: Vrij
Burgers en bedrijven waar geen concrete verdenkingen tegen bestaan moeten erop kunnen rekenen dat hun activiteiten op het Internet nimmer onderworpen zullen worden aan structureel onderzoek of analyse. Dat betekent concreet:

- Niet verzamelen van data in bulk zonder een sterke, duidelijke gerichtheid op een specifiek onderzoeksonderwerp. “Nevenvangst “ moet direct worden verwijderd.
- Geen opslag van gegevens van burgers en bedrijven die niet het onderwerp zijn van onderzoek.
- Slechts uitwisseling met andere diensten en landen van data over burgers of bedrijven waar een specifieke, gerichte verdenking tegen bestaat.

Kernwaarde: Open
Het ontbreken van degelijk toezicht, het bewust verzwakken van veiligheidssystemen, het verzamelen en uitwisselen van data van onschuldige burgers, leiden ertoe dat de opslag van data in het betreffende land niet langer wordt vertrouwd. Waar dit toe kan leiden zagen we recent: het privacy shield was nodig om data van Europese burgers te beschermen tegen ingrepen door Amerikaanse inlichtingendiensten. Nog steeds is in vele landen de roep te horen om data slechts in eigen land op te slaan. Zulke beperkingen schaden het vrije verkeer van data en diensten en maken Nederland minder aantrekkelijk als vestigingsplaats voor Internationale aanbieders. In concreto:

- Afzien van ongericht tappen, afluisteren en ingrijpen op internationale verbindingen, voorzieningen en veiligheidssystemen (knooppunten, internationale carrier verbindingen, zeekabels, veiligheidssystemen zoals TTP, generieke infrastructurele voorzieningen)

DINL. December 2016