Stichting Digitale
Infrastructuur Nederland

Maanweg 174
2516 AB, Den Haag
mvanvliet@dinl.nl

Aan: De leden van de Tweede Kamer der Staten-Generaal, Vaste Commissie voor Digitale Zaken
Datum: 10 maart 2026
Betreft: Behoud OKTT-status onder de Cyberbeveiligingswet

Geachte Kamerleden,

Wij schrijven u naar aanleiding van de behandeling van de Cyberbeveiligingswet (Cbw). Met deze brief willen wij uw aandacht vragen voor een specifiek onderdeel dat naar onze overtuiging een serieus risico vormt voor de collectieve cyberveiligheid van Nederland: het afschaffen van de OKTT-status zonder een heldere, gegarandeerde opvolger.

Een bewezen systeem staat op het spel

Onder de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) wordt dreigingsinformatie effectief gedeeld via zeven zogeheten "organisaties die objectief kenbaar tot taak" (OKTT) hebben andere organisaties of het publiek te informeren over cyberdreigingen en -incidenten. Dit zijn NBIP, Ferm-zeehavens, Cyberweerbaarheidscentrum Brainport, Cyberveilig Nederland, Connect2Trust, Circle of Trust en Abuse Information Exchange. Deze organisaties bereiken doelgroepen – waaronder cruciale toeleveranciers en het MKB – die buiten het directe bereik van het NCSC vallen. Het systeem werkt, is bewezen effectief en vormt een essentiële schakel in de informatievoorziening aan partijen die Nederland digitaal weerbaar houden.

Met de inwerkingtreding van de Cbw vervallen alle OKTT-aanwijzingen van rechtswege. In de memorie van toelichting (p. 115) wordt gesteld dat deze organisaties "onder omstandigheden" kunnen worden gekwalificeerd als "relevante partij" in de zin van artikel 16, tweede lid, onderdeel b, Cbw. Deze formulering is echter allesbehalve een garantie. Het is volstrekt onduidelijk aan welke voorwaarden een organisatie moet voldoen om als relevante partij te worden aangemerkt. Moet de gehele achterban bestaan uit essentiële of belangrijke entiteiten? Is één enkele essentiële entiteit in de achterban voldoende? De wet en de memorie van toelichting geven hier geen antwoord op en ook op basis van rechtstreekse vragen aan de NCTV en NCSC wordt dit niet duidelijk.

Onzekerheid is slecht voor cyberweerbaarheid

Die onduidelijkheid is geen juridisch-technische kwestie: zij heeft directe gevolgen voor de veiligheid van Nederlandse organisaties. Zolang niet vaststaat of huidige OKTT's dreigingsinformatie blijven ontvangen, kunnen zij hun informatievoorziening niet continueren en kunnen hun achterbannen niet tijdig worden gewaarschuwd. De recente cyberincidenten bij Odido, het OM en zorglaboratoria laten zien wat de kosten zijn van informatieachterstand en de maatschappelijke onrust die het (terecht) veroorzaakt. Voortdurende onzekerheid over de status van schakelorganisaties vergroot de kans op soortgelijke incidenten omdat straks minder organisaties relevante informatie krijgen waarop ze kunnen handelen. Uit correspondentie van een van onze leden blijkt dat specifieke informatie zoals onder andere TLP: AMBER producten en adviezen van het NCSC voor organisaties die niet onder de Cbw vallen straks niet langer beschikbaar is. OKTT organisaties die zich onder de Cbw vrijwillig registreren in het meldportaal onder de Cbw ontvangen straks dus niet dezelfde informatie die zij nu wel krijgen via de huidige OKTT route.

Tegelijkertijd wordt ingezet op nieuwe ondersteunende structuren voor informatiedeling zoals Cyclotron, waarvan de effectiviteit nog niet is aangetoond vanwege de onduidelijkheid met betrekking tot de te bereiken doelgroepen. Het is vanuit het perspectief van antifragiliteit onverstandig om bestaande, functionerende structuren te ontmantelen voordat alternatieven hun waarde hebben bewezen. Wij roepen u op niet te gokken met de digitale veiligheid van Nederland.

Kortom, geef de huidige OKTT's de zekerheid dat zij ook onder de Cbw aangemerkt zullen worden als "relevante partij" zodat zij relevante dreigingsinformatie blijven ontvangen waarmee zij bedrijven en consumenten online veilig kunnen houden.

Wij zijn graag bereid dit standpunt nader toe te lichten.

Met vriendelijke groet,

Marijn van Vliet, directeur DINL
Octavia de Weerdt, algemeen directeur NBIP
Liesbeth Holterman, directeur Cyberveilig Nederland
Raymond Bierens, voorzitter Connect2Trust
Marijn van Schoote, Managing director Ferm-zeehavens