Ministerie van **Justitie en Veiligheid**

Implementatie van Europese richtlijn voor veerkracht van kritische entiteiten (CER-richtlijn)

Bij implementatie van CER-richtlijn dient voor drinkwatersector verwezen te worden naar eisen in Drinkwaterwet- en besluit.
In Europa is de CER-richtlijn aangenomen. Doel van de richtlijn is het waarborgen van de levering van essentiële diensten in de EU door versterking van de weerbaarheid. De Nederlandse drinkwaterbedrijven vallen binnen de reikwijdte van de richtlijn. De verplichtingen die voortkomen uit de richtlijn, zijn reeds onderdeel van bestaande sectorale wetgeving, namelijk de Drinkwaterwet en het Drinkwaterbesluit. Om dubbele lasten en eventuele tegenstrijdigheden te voorkomen, dient bij de implementatie van de CER-richtlijn (via bijvoorbeeld een brede Vitaal-wet) voor de drinkwatersector verwezen te worden naar eisen in Drinkwaterwet en -besluit.
Daarnaast dient in de implementatiewet te worden geborgd dat alle vitale bedrijven in Nederland gebruik kunnen maken van de Aanbestedingswet Defensie- en Veiligheidsgebied. Deze voorziet in procedures waarbij niet allerlei gevoelige informatie naar derden openbaar hoeft te worden gemaakt bij inkoop en aanbesteden van bepaalde werken of diensten.

Europese richtlijn voor de veerkracht van kritische entiteiten (CER-richtlijn), De Aanbestedingswet Defensie- en Veiligheidsgebied
Sabine Gielens

Cybersecurity

Richt 'trusted channels' in tussen overheid en vitale sectoren.
De grootste digitale dreiging voor de veiligheid van Nederland wordt gevormd door staten. Vitale sectoren lopen door deze dreiging een grotere kans om te worden gehackt met verstoring of uitval als gevolg. Eén van de belangrijkste instrumenten om de cyberweerbaarheid van vitale bedrijven, waaronder de drinkwaterbedrijven, te verhogen, is hen te voorzien van dreigingsinformatie en inlichtingeninformatie. Snelheid is hierbij cruciaal. Juist dit soort (niet-openbare) informatie is noodzakelijk om bedrijven in staat te stellen invulling te geven aan hun verantwoordelijkheid en tijdig de nodige maatregelen te treffen om de continuïteit van de vitale dienst te borgen. Om dit mogelijk te maken pleit Vewin voor het inrichten van 'trusted channels' tussen betrokken overheidsinstanties en vitale bedrijven.
Ook pleit Vewin voor een structureel cyber-oefenprogramma van de overheid én vitale sectoren. In dit oefenprogramma moet de nadruk worden gelegd op duidelijke afstemmings- en informatielijnen en coördinatie en regie.

Economische Veiligheid, Nederlandse Cybersecurity Agenda, Nationale Veiligheid Strategie
Sabine Gielens