



# Cyberweerbaarheidsconferentie

Samen verder, samen weerbaar

Maandag 26 mei 2025

## Dagprogramma

Tijd	Activiteit
09.00-09.30 uur	<b>Inloop</b>
09.30-10.30 uur	<b>Plenaire opening</b> <i>In gesprek met de ILT, NCSC, NVWA en beleid IenW Wat doet de overheid voor jou? Begeleid door dagvoorzitter Lucinda Sterk</i>
10.30-11.00 uur	<b>Koffiebreak</b>
11.00-11.45 uur	<b>Deelsessies ronde 1</b>
11.45-13.00 uur	<b>Lunch</b>
13.00-13.30 uur	<b>Keynote</b> <i>Cyberweerbaarheid in een veranderende wereld door Peter van Uhm</i>
13.30-13.45 uur	<b>Wisselmoment</b>
13.45-14.30 uur	<b>Deelsessies ronde 2</b>
14.30-15.00 uur	<b>Koffiebreak</b>
15.00-15.45 uur	<b>Deelsessies ronde 3</b>
15.45-16.00 uur	<b>Wisselmoment</b>
16.00-16.30 uur	<b>Plenaire afsluiting</b> <i>Samen verder! door Dimitri van Zantvliet</i>
16.30-18.00 uur	<b>Borrel</b>

## Deelsessies

	Ronde 1	Ronde 2	Ronde 3
AI-impact Assessment	11.00 - 11.45 uur	13.45 - 14.30 uur	
Risicomanagement in OT cybersecurity	11.00 - 11.45 uur	13.45 - 14.30 uur	
Innovatie in cyber	11.00 - 11.45 uur		15.00 - 15.45 uur
Quantum bij IenW	11.00 - 11.45 uur	13.45 - 14.30 uur	
OT dreigingsbeeld	11.00 - 11.45 uur		
Wat voor impact hebben satellieten op jou?	11.00 - 11.45 uur		15.00 - 15.45 uur
Speel het Cyclonronspel	11.00 - 11.45 uur	13.45 - 14.30 uur	15.00 - 15.45 uur
Weerbaarheids training	11.00 - 11.45 uur		
Een gezamenlijke beveiligingsnorm voor drinkwater	11.00 - 11.45 uur		
Toezicht op cyberweerbaarheid		13.45 - 14.30 uur	15.00 - 15.45 uur
Patchen of verzuipen		13.45 - 14.30 uur	
Samenwerking in het laadinfra ecosysteem		13.45 - 14.30 uur	
Cyber tafelgesprekken		13.45 - 14.30 uur	
NIS2-college			15.00 - 15.45 uur
Hack out in de energiesector. Hoe te voorkomen?			15.00 - 15.45 uur
OT Cases			15.00 - 15.45 uur
Architectuur op orde (1,5 uur)		13.45 - 15.15 uur	
Samen weerbaar is óók luisteren naar elkaar			15.00 - 15.45 uur

Thema's: [Wat komt er op ons af?](#) [Dreigingen](#) [Hoe gaan we samenwerken?](#)

### AI-impact Assessment

Ronde 1: 11.00 – 11.45 uur  
Ronde 2: 13.45 – 14.30 uur

Deze sessie wordt gegeven door: **CDIB – Ministerie van IenW**

Er is enorm veel mogelijk met AI, maar het brengt ook risico's met zich mee. Hoe ga je om met deze risico's, terwijl je wel de kansen en mogelijkheden pakt? Voor de inkoop en ontwikkeling van een AI-systeem kun je het AI Impact Assessment (AIIA) gebruiken. Deze tool helpt bij het maken van een afweging voor het gebruik van AI en geeft een overzicht van alles waar je aan moet denken. In deze sessie gaan we in op de aanpak en wie je hierbij moet betrekken. En vooral: hoe gebruik je het AIIA zodat het zoveel mogelijk toegevoegde waarde geeft binnen een project?

### Risicomanagement in OT cybersecurity

Ronde 1: 11.00 – 11.45 uur  
Ronde 2: 13.45 – 14.30 uur

Deze sessie wordt gegeven door: **Secura BV**

Steeds meer industriële technologie wordt met elkaar verbonden. Hoe creëer je een overzicht van de meest kwetsbare systemen die je in gebruik hebt, wat kan een cybersecurity incident veroorzaken en welke risico's heeft dat voor onze bedrijfsprocessen? Effectief risicomanagement kan helpen deze vragen te beantwoorden. Deze workshop behandelt de opbouw van een risicomanagement proces, en de unieke uitdagingen die je tegenkomt als je dit proces toepast op operationele technologie.

### Innovatie in cyber: wat brengt de toekomst?

Ronde 1: 11.00 – 11.45 uur

Deze sessie wordt gegeven door: **Intersect**

In drie korte gesprekken nemen we jullie mee door de ontwikkelingen van cyber op dit moment. Op een toegankelijke manier praten we over de nut- en noodzaak van resilience-by-design. Welke gevaren heb je nog niet goed in beeld? Welke maatregelen kan je nemen? En zijn die technisch of meer organisatorisch van aard? Ontdek het samen met de mensen van het NWO INTERSECT programma.

### Toezicht op cyberweerbaarheid: wat betekent dit in de praktijk?

Ronde 1: 11.00 – 11.45 uur  
Ronde 3: 15.00 – 15.45 uur

Deze sessie wordt gegeven door: **Inspectie Leefomgeving en Transport (ILT)**

Je wordt ondersteund bij het vormgeven van je cyberweerbaarheid. Denk bijvoorbeeld aan het IenW Cyberweerbaarheidsprogramma, ISACS en CSIRTS. Je hebt echter ook recht op toezicht. Hoe wordt dit vormgegeven en wat wordt er van je verwacht? Leer er meer over tijdens deze sessie.

### NIS2-college: risicomanagement en best practices

Ronde 3: 15.00 – 15.45 uur

Deze sessie wordt gegeven door: **EY**

Tijdens dit NIS2-college behandelen we de vereisten vanuit de NIS2 Directive, zodat organisaties weten wat van hen verwacht wordt en welke maatregelen ze moeten nemen. De focus ligt hierbij op risicomanagement en de best practices daarin.

**Quantum bij IenW**Ronde 1: 11.00 – 11.45 uur  
Ronde 2: 13.45 – 14.30 uur**Deze sessie wordt gegeven door: CDIB – Ministerie van IenW**

Quantumtechnologie brengt revolutionaire kansen, maar ook dreigingen met zich mee. Als sleuteltechnologie is het essentieel om de impact op in kaart te hebben en daar tijdig op te acteren. CDIB houdt zich sinds 2021 bezig met het voorbereiden op potentiële dreigingen (en kansen) voor IenW. In deze sessie vertellen Frederik Kerling (Senior Consultant Quantum van TNO) en Loulou Hanna (Adviseur AI en Quantumtechnologie CDIB IenW) je meer over quantum en wat het in de nabije toekomst ligt.

**OT Dreigingsbeeld**

Ronde 1: 11.00 – 11.45 uur

**Deze sessie wordt gegeven door: NCSC**

Steeds vaker is operationele technologie (OT) het doelwit van cybercriminelen en andere kwaadwillende actoren. Gelukkig kun je het risico op een cyberaanval verkleinen met de juiste kennis en maatregelen. Het NCSC speelt hierbij een onmisbare rol. Een dreigingslandschap is een verzameling van inzichten die we binnen het hele landschap van dreigingen waarnemen. Deze inzichten verwerken ze in een product: een dreigingsbeeld dat organisaties helpt om zich beter voor te bereiden op cyberdreigingen.

**Wat voor impact hebben satellieten op jou?**Ronde 1: 11.00 – 11.45 uur  
Ronde 3: 15.00 – 15.45 uur**Deze sessie wordt gegeven door: S&T [Science & Technology]**

Plaats en tijdsbepaling is voor velen een vrij abstract begrip. Menigeen denkt niets of weinig te merken van een uitvallende satelliet. Maar wat als we GPS niet meer betrouwbaar kunnen gebruiken? In deze break-out sessie nemen André en zijn collega('s) van het GNSS Centre of Excellence u mee in de wereld van GPS en andere vormen van plaats- en tijdsbepaling met behulp van satellieten. Ze leggen uit hoe verweven onze systemen met deze satellieten zijn; wat er gebeurt wanneer we geen controle meer hebben over deze satellieten; en waar we aan moeten denken om de impact te minimaliseren.

**Hack out: hoe cyber criminelen het elektriciteitsnet kunnen verstoren en hoe wij dat helpen te voorkomen.**

Ronde 3: 15.00 – 15.45 uur

**Deze sessie wordt gegeven door: HVC DIVD**

Het Europese elektriciteitsnetwerk is een smart grid geworden. Steeds meer apparaten zijn slim en online verbonden met elkaar. Dat geeft veel kansen, maar maakt ons energiesysteem ook kwetsbaarder voor digitale aanvallen. In een tijd van toenemende dreiging van hybride oorlogsvoering zullen we er rekening moeten houden dat ineens het licht uitgaat. In deze presentatie laat onderzoeker Chris van 't Hof zien hoe een hack-out technisch in zijn werk gaat. Hij neemt ons mee in een duister scenario, maar laat ook zien hoe we dat kunnen voorkomen door samen kwetsbaarheden te vinden en die op te lossen.

**Patchen of verzuipen**

Ronde 2: 13.45 – 14.30 uur

**Deze sessie wordt gegeven door: Yunex Traffic**

Wat is er nodig op het moment dat er een kritieke vulnerability gevonden is om toch tot een veilige vitale water infrastructuur te komen? Hoe maak je de afweging tussen veiligheid en beschikbaarheid? Tijdens deze presentatie nemen we de luisteraar mee in het spanningsveld tussen enerzijds cyber veilig zijn en anderszijds zorgen dat de operationele infrastructuur niet vast loopt.

**OT cases: aanvalsroute en maatregelen**

Ronde 3: 15.00 – 15.45 uur

**Deze sessie wordt gegeven door: EY**

In deze deelsessie behandelen cybercrises gerelateerd aan OT die in de recente historie hebben plaatsgevonden. We gaan per case de diepte in op de aanvalsroute en de defensieve maatregelen die de organisaties hebben genomen.

**Speel het Cyclotron spel:  
Samenwerken voor een  
cyberveilig Nederland**

Ronde 1: 11.00 – 11.45 uur  
Ronde 2: 13.45 – 14.30 uur  
Ronde 3: 15.00 – 15.45 uur

**Deze sessie wordt gegeven door: NCTV en NCSC**

Het programma Cyclotron is een publiek-private samenwerking tussen overheid, bedrijven en maatschappelijke organisaties. Dit heeft geleid tot een platform bij het NCSC waarbinnen informatie wordt gedeeld over digitale incidenten en dreigingen. Door gezamenlijke analyse en distributie van geanalyseerde gegevens helpen deze organisaties Nederland een onaantrekkelijk doelwit te maken voor digitale aanvallen. In het spel dat we hebben ontwikkeld ervaren partijen hoe het is om echt samen te werken. Als je dat goed doet, bereik je meer dan dat je alleen kan!

**Cyberbeveiliging van  
drinkwaterbedrijven: een  
gezamenlijke beveiligingsnorm  
voor het kloppende hart van  
de drinkwatervoorziening  
- NIS2-proof.**

Ronde 1: 11.00 – 11.45 uur

**Deze sessie wordt  
gegeven door: Vewin**

Onder de Wbni hebben de drinkwaterbedrijven een gezamenlijke beveiligingsnorm voor de PA opgesteld. Met de komst van de Cbw en Wwke wordt deze norm geüpdatet om te voldoen aan de nieuwe scope en wet- en regelgeving. De focus van deze norm ligt op het aantoonbaar voldoen met een behapbare auditdruk voor de drinkwaterbedrijven en het bijdragen aan de beveiliging van de organisatie. Deze norm wordt zowel intern als extern geaudit en de resultaten worden met de toezichthouder gedeeld. Deze manier van werken nemen we mee voor het bereiken van het volgende niveau (NIS2). Deze deelsessie neemt je mee in de samenwerking en totstandkoming van deze norm.

**Weerbaarheidstraining,  
maar dan net even anders...**

Ronde 1: 11.00 – 11.45 uur

**Deze sessie wordt gegeven door: Provincie Gelderland**

Heb jij ook zo'n hekel aan verplichte eLearning modules? Herkenbaar, dat hebben onze medewerkers ook. Daarom kiezen wij bewust voor een persoonlijke aanpak. Digitale Weerbaarheid 2.0 hebben wij zelf ontwikkeld, op basis van praktijk cases uit onze organisatie. Ervaar deze training zelf, en doe inspiratie op voor je eigen organisatie, jouw collega's zullen je dankbaar zijn...

**Architectuur op orde: De  
PA cyberweerbaarheid  
vergroten met behulp  
van zones en conduits**

Ronde 2|3: 13.45 – 15.45 uur  
Let op: duurt 1,5 uur. Geen  
andere sessie in Ronde 3.

**Deze sessie wordt gegeven door: KienIA**

De sessie begint met korte introductie op het Zones & Conduits model: Wat is het en hoe stel je deze samen? Aan de hand van 2 concrete praktijkvoorbeelden bij de waterschappen kijken we hoe het model heeft geholpen om de benodigde inzichten te verkrijgen en de PA meer in control brengen. Beide praktijkvoorbeelden worden besproken waarbij het publiek de mogelijkheid heeft om verdiepende vragen te stellen. We moedigen interactie dan ook ten zeerste toe.

**Cyberweerbaarheid door  
samenwerking in het  
laadinfra ecosysteem**

Ronde 2: 13.45 – 14.30 uur

**Deze sessie wordt gegeven door: Eviolin**

Hoe werk je effectief samen aan cyberweerbaarheid in een ecosysteem dat volop in ontwikkeling is? In deze sessie deelt Eviolin – een samenwerkingsverband van diverse aanbieders van laadinfrastructuur – hoe zij samen met hun leden bouwen aan een veerkrachtig laadinfra-netwerk. In deze sessie worden praktijkvoorbeelden en incidenten besproken. Hierbij is extra aandacht voor uitdagingen in samenwerking, zoals het delen van informatie en het creëren van vertrouwen. Op basis van deze concrete situaties gaan we samen in gesprek: welke drempels herken je, en hoe kunnen we de samenwerking binnen dit jonge maar kritieke domein versterken?

**Samen weerbaar is óók  
luisteren naar elkaar**

Ronde 3: 15.00 – 15.45 uur

**Deze sessie wordt gegeven door: IenW**

Alleen kom je ver, maar samen kom je verder. Een quote die je vaak hoort, maar hoe geef je hier nou invulling aan? Vanuit het ministerie van IenW hebben wij luistertafels beschikbaar. Luisteren is een kunst. Een hele belangrijke kunst! Want door te luisteren kan je begrip krijgen voor een ander. Graag horen wij waar het cyberweerbaarheidsprogrammering van IenW op kan inspelen. Heb je een nieuw initiatief? Of wil je gewoonweg wat meegeven aan ons? Je bent welkom bij de luistertafels van het ministerie van IenW.

Cyber tafelgesprekken

Ronde 2: 13.45 – 14.30 uur

Deze sessie wordt gegeven door: **IenW**

Deze interactieve sessie biedt een unieke kans om je inzichten te verrijken door in kleine groepen over actuele cyberveerbaarheidsvraagstukken van gedachten te wisselen. De dynamiek aan de tafels stimuleert samenwerking, kennisdeling, en helpt je om waardevolle connecties te leggen met professionals uit diverse sectoren. Door direct in dialoog te treden met vakgenoten, ontdek je nieuwe perspectieven en innovatieve oplossingen die je in je dagelijkse werk kan toepassen. Mis deze unieke gelegenheid niet om samen met andere experts de fundamentele van cyberveiligheid te verkennen en te verbeteren.

