



Aanpak van statelijke dreigingen

De aanpak van statelijke dreigingen is gericht op het beschermen van onze mensen, infrastructuur en informatie.

Het kabinet zet in op een integrale, maatschappijbrede aanpak samen met alle publieke en private partners. Hiermee wordt een systematiek en manier van samenwerken ontwikkeld die per casus op maat kan worden gemaakt. De aanpak kent de volgende elementen:

Invoeren vaste werkwijze

Het *identificeren* van belangen, het *signaleren* van dreigingen, en het *stimuleren* van de weerbaarheid.

Verbeteren informatiepositie en informatiedeling

Het tijdig zicht krijgen op en duiden van (potentiële) dreigingen met (inter)nationale partners.

Stimuleren bewustwording

Bij overheden, diplomaten, CEO's van vitale en private partners, en het algemene publiek.

Vergroten kennis

Om kennis over weerbaarheid tegen statelijke dreigingen te vergroten.

Inzetten maatregelen ter verdediging

Zoals diplomatieke instrumenten en verkenning naar registratieplicht lobbyisten.

Verbinden economie en veiligheid

Investeringsstoets op nationale veiligheid, vergroten bewustwording bij rijk en vitale sectoren van risico's bij inkoop en aanbesteding, inzet op beschermen kritieke technologie.

Verbeteren digitale aanpak

Gericht op robuuste infrastructuur, weerbaarheid en digitale slagkracht zoals verwoord in de Nederlandse Cybersecurity Agenda (NCSA).

Internationaal samenwerken

Bevorderen internationale rechtsorde, optimale samenwerking met EU, NAVO en andere instellingen.

