Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Ontwrichting van de maatschappij ligt op de loer

Grootste dreiging is spionage, verstoring en sabotage vanuit statelijke actoren.

Landen als China, Iran en Rusland hebben offensieve cyberprogramma's gericht tegen Nederland.

Dit betekent dat deze landen digitale middelen inzetten om geopolitieke én economische doelstellingen te bereiken ten koste van Nederlandse belangen. Verstoring en sabotage hebben de meeste impact op de nationale veiligheid.

Vrijwel alle vitale processen en diensten zijn volledig afhankelijk van ict.

Afhankelijkheid van gedigitaliseerde processen en systemen is zo groot geworden dat aantasting kan leiden tot maatschappij-ontwrichtende schade.

Terugvalopties en analoge alternatieven zijn vrijwel afwezig. Vanwege de omvang van de dreiging en het achterblijven van de weerbaarheid, ontstaan risico's voor de nationale veiligheid.

Cybersecuritybeeld Nederland 2019

Het CSBN biedt inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid.

Weerbaarheid niet overal op orde.

Weerbaarheid belangrijkste instrument om risico's te verminderen, want beïnvloeden dreiging en afhankelijkheid blijkt complex.

Maatregelen worden niet altijd genomen omdat de kostendrager niet altijd de baten ervaart. Onveilige producten en diensten vormen een achilleshiel voor de digitale veiligheid. Nederland is afhankelijk van een beperkt aantal aanbieders en landen. Dit maakt ons kwetsbaar voor veranderende intenties.

Het CSBN is een jaarlijkse publicatie van de NCTV en komt tot stand in samenwerking met publieke en private partners, en de wetenschap.

Lees het hele CSBN op **www.nctv.nl**