



Algemene Inlichtingen- en  
Veiligheidsdienst  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties



CHINA SCIENCE  
INVESTIGATION

20 MEI 2022 · ⌚ 13 MIN.

**China stuurt gericht tientallen militaire  
onderzoekers naar Nederland om  
gevoelige kennis te vergaren**

10

# STATELIJKE ACTOREN & KENNISVEILIGHEID

30 juni 2022



## KENNISVEILIGHEID

Nu een actueel onderwerp maar al langer op de agenda zij het op kleine schaal, eerder vooral gericht tegen Iran (Iraanse studenten en) vervolgens ook op N-Korea.

Steeds meer oog voor risico vanuit China

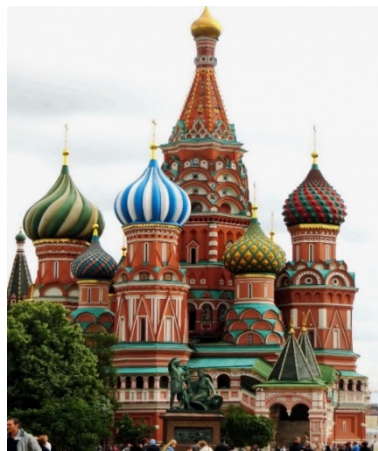


De samenwerking van Nederlandse universiteiten met de Chinese krijgsmacht beperkt zich niet tot militaire universiteiten. De afgelopen zeven jaar zijn er ook vele honderden onderzoeken gedaan met civiele Chinese universiteiten die zelf voor het leger werken.



## SITUATIE

- Nederland is interessant voor het vergaren van inlichtingen op het gebied van hoogtechnologische doeleinden.
- Statelijke cyberactoren voeren cyberoperaties uit tegen Nederlandse instellingen, ook kennisinstellingen kunnen hiervan het doelwit zijn.
- Samenwerkingsverbanden met Nederlandse kennisinstellingen





## WENSENLIJST STATELIJKE ACTOREN

Algemeen: - Data  
- Persoonsgegevens

Technologieën: - High tech  
- Landbouw-  
- Agro-  
- Energie  
- Militair

Beleid: - Buitenlands beleid  
- Migrantenbeleid t.a.v.  
eigen gemeenschappen

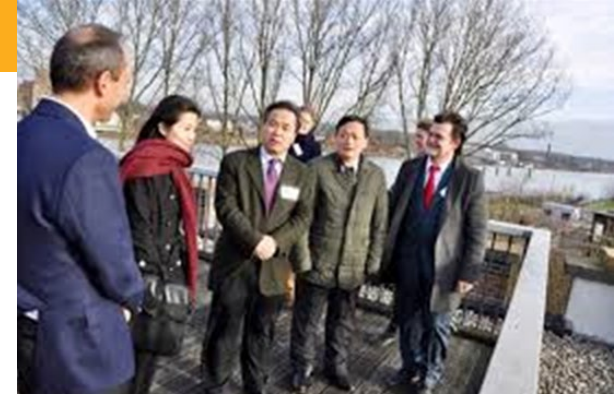
Overig: - Aangrijpingspunten  
- Kansen voor indringing /  
stepping stones  
- Zwakke plekken



# ONGEWENSTE KENNISOVERDRACHT

Verschillende vormen:

1. Exploitatie van samenwerking en legale kennisdeling
2. Spionage
3. Cyber





## MOGELIJKE SCHADE VOOR KENNISINSTELLINGEN

Verlies data

Verlies kennispositie

Verlies wetenschappelijke voorsprong

Verlies IP

Verlies of modificatie onderzoeksgegevens

Beïnvloeding onafhankelijkheid instelling

Beïnvloeding onderzoek

Medewerking aan proliferatie

Medewerking aan militaire kennisopbouw

Militair gebruik van civiele vindingen

Betrokkenheid ethisch/morele kwesties

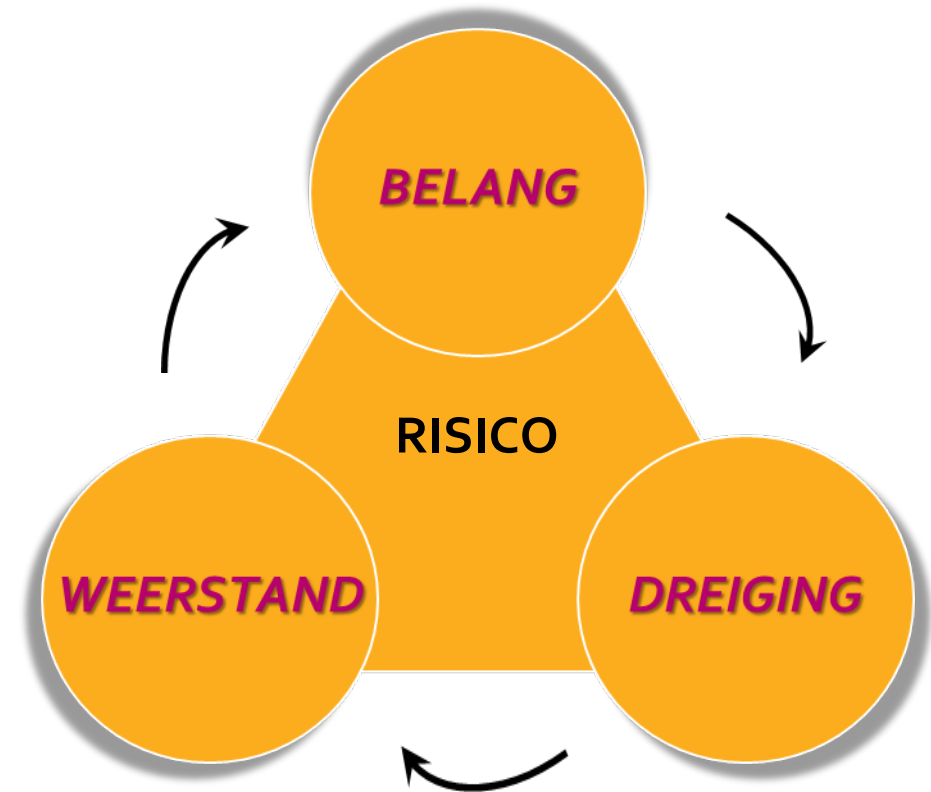


## PREVENTIE: WAT KUNNEN WE DOEN?

WELKE?

tegen WIE of WAT?

HOE?



Het meest effectief is de combinatie van technische én gedragsmaatregelen



# PREVENTIE

Bewust gebruik van apparatuur



ICT: basis op orde



Check voor je connect



Interne ethische code



Awareness

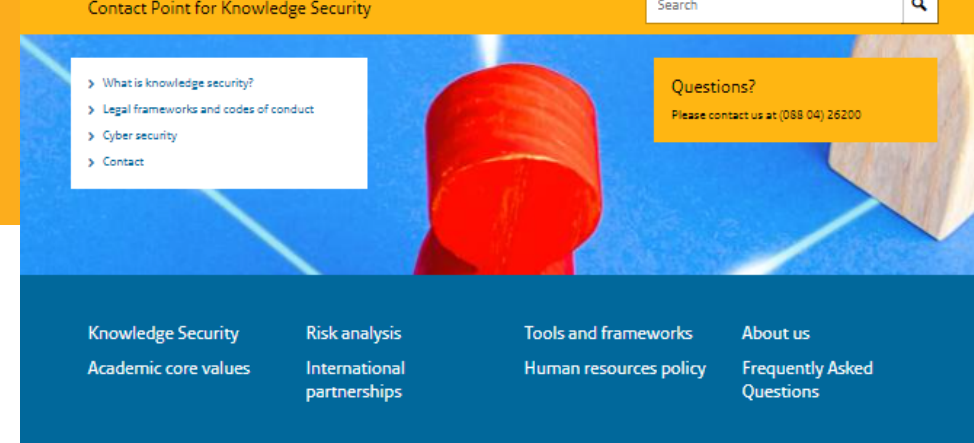






# PRAKTISCH: LOKET KENNISVEILIGHEID

- Loket en IRK
- Vragen en meldingen
- Reactietermijn, intern en extern, naslag en advies
- CV, onderzoek, behoeftestelling
- Relevantie voor Chinadossiers
- Afwegingskader



The National Contact Point for Knowledge Security is a collaboration between different Dutch ministries, and offers help to anyone connected to a knowledge institution with questions about opportunities, risks and practical matters concerning international cooperation.



## News

[New: English website of National Contact Point for Knowledge Security](#)  
22-04-2022 | 00:00

The English website of the National Contact Point (NCP) for Knowledge Security was launched today. Check out the website.

[Frequently asked questions about cooperation with Russian Federation and Belarus](#)  
22-03-2022 | 00:00

The National Contact Point for Knowledge Security has seen an increase in the number of questions from knowledge institutions ...

[> More news](#)





## NABIJE TOEKOMST KENNISVEILIGHEID

- Paradigmaverschuiving
- Blacklist en risicovakgebieden?
- Kennisveiligheidsdialogen 2.0 en risicoanalyses
- Studenten, onderzoekers en kennismigranten
- MIVD en kennisveiligheid
- Dreigingsinschatting kennisveiligheid?
- Loket en toetsingseenheid economische veiligheid?



# SAMENVATTING

Statelijke actoren *spioneren* dagelijks in Nederland,  
door *cyberaanvallen* en *menselijke bronnen*,  
bij overheid, *kennisinstellingen* en  
bedrijfsleven.

Door *veiligheidsbewustzijn*, de juiste  
*maatregelen* en *gewenst gedrag*,  
gericht op de *te beschermen belangen*,  
kan de *weerbaarheid* hiertegen worden  
verhoogd.



# Dank voor uw aandacht

Algemene Inlichtingen- en Veiligheidsdienst

Telefoonnummer: 079-3205050