# CYBERDREIGINGSBEELD 2025

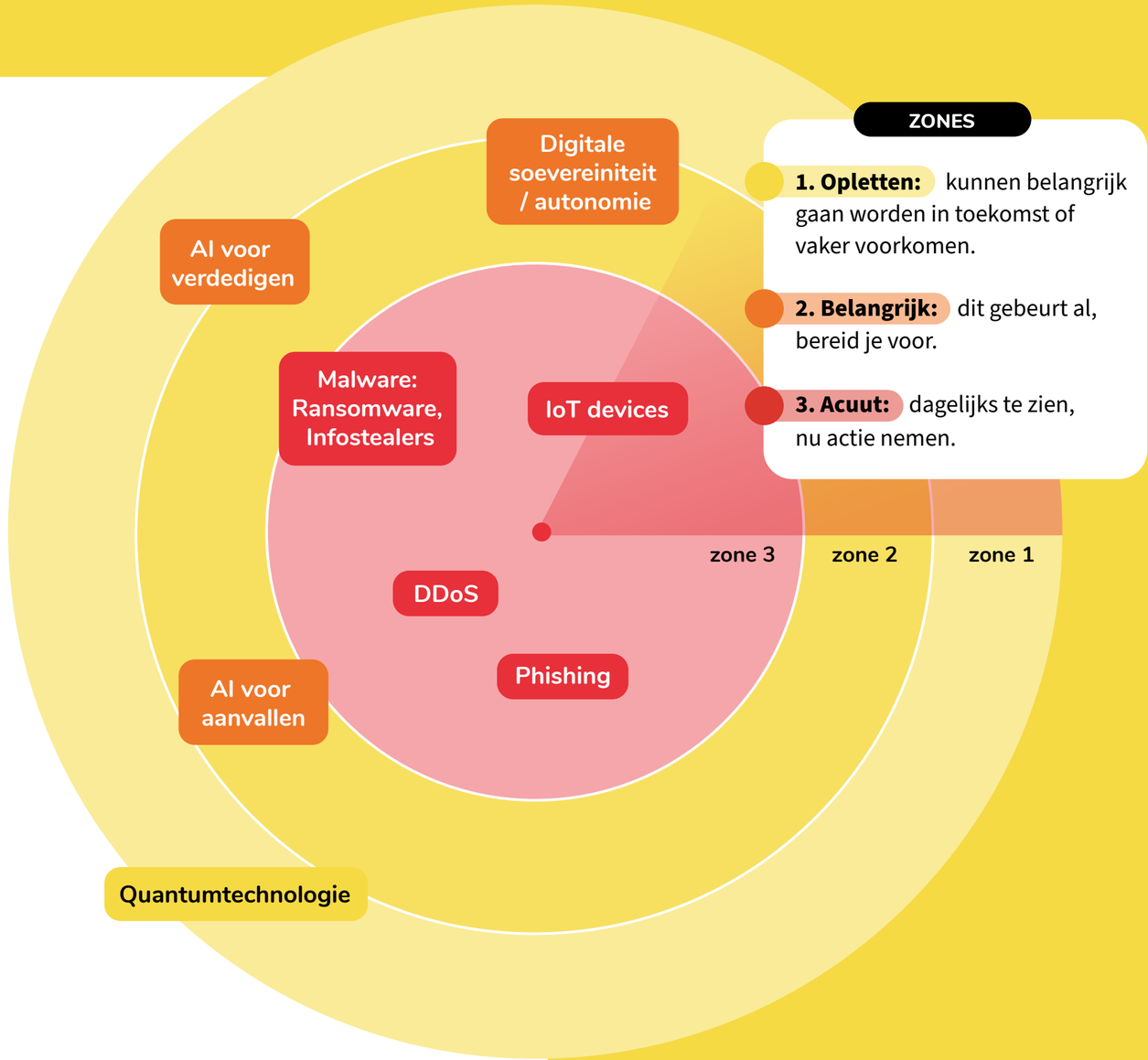
De belangrijkste cybersecuritytrends en -dreigingen in onderwijs en onderzoek


SURF

# TOELICHTING DREIGINGEN

In 2025 zien we soortgelijke dreigingen als in voorgaande jaren. Een aantal trends springen er uit:

- **DDoS, malware (infostealers, ransomware)** en **phishing** zijn en blijven de meest relevante dreigingen.
- Malware richt zich op allerlei systemen, maar vooral **IoT-devices** zijn kwetsbaar. Steeds meer van dit soort apparaten hangen aan het netwerk en onderhoud gebeurt niet structureel, waardoor ze een risico vormen.
- De **opkomst van AI** heeft een kantelpunt gecreëerd in het dreigingslandschap van cybercriminaliteit. Het maakt het voor kwaadwillenden eenvoudiger, effectiever en efficiënter om aanvallen uit te voeren.



We zien dat **AI** in toenemende mate een centrale rol speelt in de ontwikkeling en samenhang van dreigingen en aanvalsmethoden:

- Zo zien we een toename van *scraper bots*, die met behulp van AI automatisch websites doorzoeken en gegevens verzamelen. Dat kan leiden tot DDoS-achtige effecten in de vorm van onbereikbare systemen en websites.

- Phishing en andere vormen van social engineering worden met hulp van AI niet alleen makkelijker, maar ook geavanceerder. Denk aan deepfakes en voice-cloning. Medewerkers en of studenten worden hierdoor nog makkelijker verleid om naar malafide websites te gaan of om inloggegevens te delen.

Tegelijkertijd wordt AI ook positief ingezet voor defensieve doeleinden. Moderne SOCs en SIEM-systemen maken steeds vaker gebruik van AI om grote hoeveelheden data real-time te analyseren, afwijkend gedrag te detecteren en sneller te reageren op incidenten.

AI speelt dus aan beide kanten van de strijd een sleutelrol.

## Uit de praktijk

- Cyberaanval Technische Universiteit Eindhoven, vijf geleerde lessen
- Hoe bescherm je je instelling tegen een DDoS-aanval?
- Simuleer een aanval op je instelling met echte dreigingen

# UITDAGINGEN VOOR DE TOEKOMST

## Digitale soevereiniteit en autonomie

Onverwacht geen toegang meer hebben tot data is in de huidige geo-politiek een reëel scenario. Als data niet beschikbaar is, vormt dat een bedreiging voor de continuïteit van onderzoek en onderwijs en kan leiden tot maatschappelijke ontwrichting. Het is belangrijk om in de SURF-coöperatie te blijven nadenken over hoe we hier mee omgaan.

▶ **Lees meer over digitale soevereiniteit en autonomie**

## Quantumtechnologie

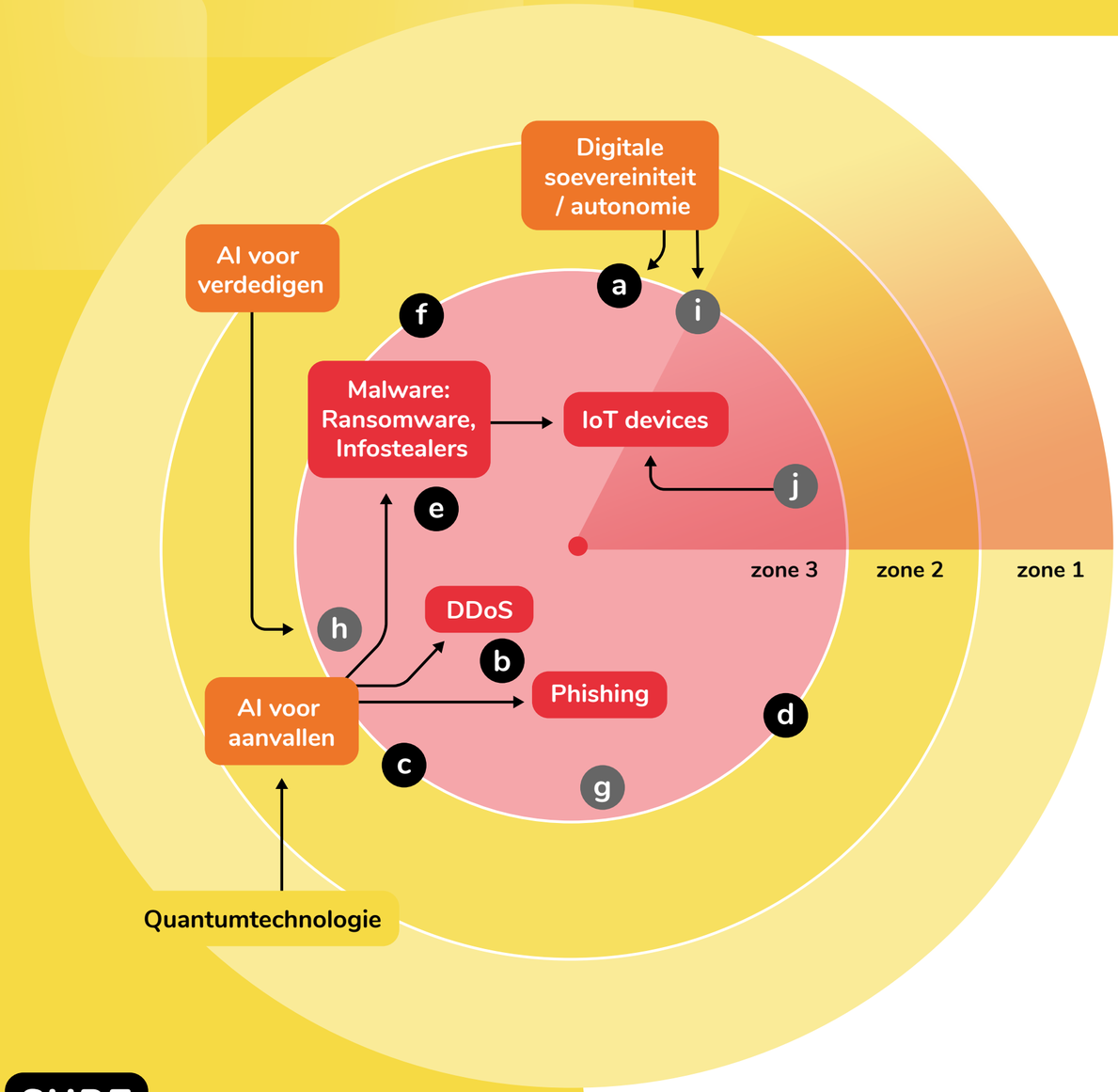
Quantumtechnologie is één van de grootste aanjagers van digitale verandering in de komende tien jaar. De kansen voor onderzoek zijn enorm, maar de impact op digitale veiligheid is minstens zo groot. Experts verwachten dat de dag waarop quantumcomputers de huidige encryptie kunnen kraken, Qday, rond 2030 zal zijn. Toch zijn risico's vandaag al aanwezig.

▶ **Bereid je voor op Qday**


### Lees alle cybersecuritytrends in het SURF Tech Trends-rapport

In het hoofdstuk Cybersecurity van het SURF Tech Trends-rapport 2026 vind je een overzicht van de belangrijkste technologische cybersecuritytrends die onderwijs en onderzoek beïnvloeden.

▶ **Download het hoofdstuk Cybersecurity**




## SAMENHANG CYBERDREIGINGEN

De uitgelichte trends staan niet op zichzelf. Vaak hangen ze samen met andere dreigingen. In het figuur geven de pijlen aan welke dreigingen vaak met elkaar samenhangen.

### Andere dreigingen:

- **a.** Spionage
- **b.** Hacktivisme
- **c.** Identiteitsfraude
- **d.** Manipulatie van data
- **e.** Overname en misbruik ict
- **f.** Verkrijging en openbaar-making van informatie

### Andere factoren die van invloed zijn op de cyberweerbaarheid:

- **g.** Awareness en gedrag
- **h.** Capaciteitstekort
- **i.** Ketenafhankelijkheid
- **j.** Kwetsbaarheden in software

### Actueel overzicht trends en dreigingen

Zie voor een actueel overzicht van van deze en andere trends en dreigingen het cybersecurity-dashboard.

▶ **Naar het SURF cybersecurity-dashboard**
(inloggen met SURFconext)

# WAT KUN JE DOEN?

## De basis op orde

De vijf algemene basisprincipes blijven essentieel om je te beschermen tegen de dreigingen en om de schade van incidenten te beperken:

- **Breng IT-risico's in kaart en stel prioriteiten voor bedrijfscontinuïteit**
- **Bevorder (awareness over) veilig gedrag**
- **Bescherm systemen, applicaties en apparaten**
- **Beheer toegang tot data en diensten**
- **Bereid je voor op incidenten**

## Meer specifieke maatregelen

Ook specifieke maatregelen als asset management, MFA, patch-management en detectie dragen bij aan de weerbaarheid van onderwijs en onderzoek.

## Direct aan de slag?

Op het SURF Security Expertise Centrum vind je praktische handreikingen en diverse templates waarmee je direct aan de slag kunt.

▶ **Naar het Security Expertise Centrum**

Oktober 2025

**SURF cybersecurity-dashboard**
Actueel overzicht trends en dreigingen

Op het SURF cybersecurity-dashboard vind je een actueel overzicht van dreigingen en trends in onderwijs en onderzoek. Het dashboard is alleen toegankelijk voor leden van de SURF Community voor Informatiebeveiliging en PRivacy (SCIPR).

▶ **Naar het SURF cybersecurity-dashboard**
(inloggen met SURFconext)