

Factsheet dreigingsbeeld n° 11

1 januari 2024-2025



Omgaan met dreiging

Een dreigingsniveau op nationaal niveau geeft een algemeen beeld over de potentiële dreiging in Nederland: 1: minimaal, 2: beperkt, 3: aanzienlijk, 4: substantieel en 5: kritiek. Voor een toelichting op de dreigingsniveaus: zie bijlage 1, uitleg nationale dreigingsniveaus. Dreigingsniveaus worden vastgesteld door de minister van Veiligheid en Justitie. Het dreigingsniveau hoeft niet altijd overeen te komen met de mogelijkheid dat een dreigingsmelding bij de VU kan binnenkomen. De eigen verantwoordelijkheid van de VU blijft belangrijk. Daarom is het belang om het lange termijn beleid uit te blijven voeren voor een goede voorbereiding op een mogelijke dreiging (zie bijlage 1 en 2 acties VU CIV), ook bij een laag landelijk dreigingsniveau.

Wat zijn de directe gevolgen van een dreiging?

De directe gevolgen van een dreiging zijn niet goed vooraf in te schatten. Dreigingen zijn vaak 'niet echt'. De context is bepalend. Het advies van de politie is hierbij van belang. De overheid kan beveiligingsmaatregelen nemen om personen en organisaties te beschermen die het doelwit kunnen worden van aanslagen. Dit verkleint het risico op terroristische aanslagen. Diverse scenario's kunnen van toepassing zijn (zie o.a. gerelateerde factsheets 'ontruimen', 'schuilen', 'bommelding', 'extreem geweld' en 'orde incidenten'). Ook kan het zinvol zijn om nog geen rechtvaardigheid te geven aan een binnengekomen dreiging ('klein' houden van de melding), maar wel om intern maatregelen te nemen. Zie hiervoor de *checklist 'omgaan met dreiging'*.

Welke vormen van dreiging zijn mogelijk?

- (acuut) zorgwekkend gedrag (zie bijlage 3);
- dreiging voor personen;
- (steek)wapen aanwezig;
- daadwerkelijk dreiging met een wapen (zie factsheet 10);
- dreiging in de (directe)omgeving VU / Zuidas / campus;
- bomdreiging of bommelding (zie factsheet 7).

Hoe kan een dreiging binnenkomen?

Het is niet waarschijnlijk dat bij een dreiging een willekeurig persoon wordt gebeld binnen de VU. Wel kan er via o.a. sociale media, politie, NCTV (via contactpersonen bij de VU) een dreigingssignaal binnenkomen. Voor een concrete dreiging: zie de *gerelateerde factsheets*. Mogelijk kunnen er (meerdere) meldingen via verschillende wegen binnenkomen.

Wie wordt direct gewaarschuwd

In geval van een dreigingsmelding moeten gewaarschuwd worden (via AC MBC of onderling bellen):

- Security desk, Hoofd beveiliging (contactpersoon politie/112);
- directeur FCO (tevens contactpersoon AIVD) en Hoofd BHV;
- OCT én SBT (*opschalingsniveau 3*).

OCT verdeelt taken onderling. De directeur FCO kan zo nodig de dreigingsmelding verifiëren bij AIVD/NCTV.

Preventief kunnen gewaarschuwd worden door OCT :

- directeuren van eenheden waar een dreiging wordt verwacht;
- AC MBC (via chef van de wacht);
- Op bestuursniveau: UvA, VUmc en ACTA, parkeerbedrijf;
- Kinderdagverblijf Kinderrijk;
- politie via contactpersoon/wijkagent;
- teamleider security desk;
- derden binnen de VU (catering, schoonmaak, winkels / horeca, foodtrucks etc.).

Inschatting ernst

Hoofd beveiliging (of plv.) stemt af met politie en doet een inschatting van de ernst van de situatie, bekijkt NCTV site (dreigingsbeeld). Hoofd beveiliging kan *Expertteam Zorgwekkend gedrag* inschakelen. Zorgen voor een gedeelde beeldvorming bij OCT en SBT. Reële scenario's nagaan (zie checklist 'omgaan met dreiging'). Alleen als wijzigingen in het dreigingsniveau leidt tot gevolgen wordt het CvB/SBT op de hoogte gebracht.

Taken crisisteam (OCT en SBT)

OCT:

- OCT komt naar de VU indien nodig;
- Nagaan rol (deel van) de BHV/VURIT (bv. stand-by, kritische Gebouw- en terreindelen afzetten, wel/niet ontruimen etc.);
- Deelt beeldvorming met SBT;
- Gaat na of er preventief *ontruimt/geschuld* moeten worden, *paniek zo veel mogelijk voorkomen*;
- Gaat de (potentiële) effecten na op de primaire processen;
- Legt de gebeurtenissen zoveel mogelijk systematisch vast.

SBT:

- SBT-kern beslist wie deelneemt aan het SBT;
- Staat 'stand-by', komt zo nodig periodiek bijeen;
- Legt contact met gemeente Amsterdam (de 'driehoek', info uitwisseling en dreigingskader vaststellen);
- Besteedt (veel) aandacht aan (pro-actieve) crisiscommunicatie en zichtbaarheid CvB;
- Gaat zorgvuldig om met (grote) bijeenkomsten, heroverwegen daarvan, gaat plannen bijeenkomsten na;
- *Onderwijs*: bespreekt hoe om te gaan met het onderwijs (stopzetten, studenten waarschuwen niet naar VU te komen, nadenken over hervatting, hoe en wanneer). Wees helder in het beleid en volg bestaande regelingen zo veel mogelijk.
- *Informereren*: bepalen hoe medewerkers en studenten blijvend en gericht geïnformeerd worden over afwikkelingen.
- *Evalueren en leren*: Maak een eigen feitenreconstructie t.b.v. de evaluatie, verantwoording en verbetering.

Communicatie

Communicatie is ALTIJD betrokken bij oproep OCT en SBT.

- Hou regie over de communicatie (C&M Crisiscommunicatieplan);
- Breng in beeld wie allemaal betrokken zijn en aandacht vragen ('stakeholderanalyse'). Geef alleen feiten weer ('*we weten het nog niet, wij zijn er en wij zijn hard aan de slag*'). Communiceer de crisis ook weer tot een einde;
- Communicatie zo mogelijk afstemmen met de gemeente/Zuidas. Zowel de boodschap, timing als afzender;
- Stem informatiestromen af en verwijst actief naar elkaar door;
- Wees alert op beeldvorming en samenhang tussen VU en VUmc (gescheiden organisaties).

Taken VURIT-BHV en beveiliging

LET OP EIGEN VEILIGHEID! BHV-ers en beveiliging. De taken bestaan alleen uit het op afstand houden van toeschouwers/ nieuwsgierigen c.q. het afzetten van het gebied i.s.m. de beveiliging/politie en ondersteunende taken (denk aan logistieke ondersteuning). Preventief ontruimen of afsluiten/afzetten van omliggende gebouwen (zie factsheet 5 'Ontruimen' en 6 'Schuilen') kan daarbij een maatregel zijn. EHBO inzet *in veilig gebied* iom. politie kan noodzakelijk zijn. De inzetpost/verzamelplaats (niet op de plek van het incident) wordt via de AC MBC aan de portofoondragers doorgegeven.

Afschaling, praktische afhandeling:

De ploegleider informeert betrokkenen zoals BHV over de afloop van het incident. Overleg tussen o.a. beveiliging en politie over aangifte en verdere afhandeling van het gebeuren. Debriefing van de acute fase met OCT en SBT.

Vooruitblik nazorgfase:

OCT en SBT maken hiervoor vervolgspraken. Nagaan of bepaalde groepen extra aandacht behoeven. Zie voor nazorg factsheet 10.

Bijlagen:

1. Uitleg nationale dreigingsniveaus en acties VU
2. Checklist terrorisme scenario's gemeente Amsterdam
3. WAVR instrument dreigingscasuïstiek

Gerelateerde BNO factsheets:

- Factsheet 5 Ontruimen
- Factsheet 5A Inrichting opvangpunt
- Factsheet 5B Ontruimen door docenten
- Factsheet 6 Schuilen
- Factsheet 7 Bommelding
- Factsheet 8 Orde incident / bedreigingen / onveilig gevoel
- Factsheet 9 Bezetting
- Factsheet 10 Extreem geweld
- Factsheet ALARM alarmering
- Factsheet Com Communicatie

Checklist 'omgaan met dreiging' (zie ook bijlage 2, Checklist terrorisme scenario's)

Deze checklist is alleen van toepassing voor dreigingsniveau 3 (als daar direct aanleiding voor is) en dreigingsniveaus 4 en 5, en voor overige dreigingssituaties waar een dreigingsgevoel van uitgaat. De checklist kan gebruikt worden om na te gaan welke (opschaling van) maatregelen nodig is voor de VU. De context van de dreiging is van belang om in te schatten welke maatregelen zinvol zijn.

Contacten:

1. Is er aanleiding voor zorg? (voor medewerkers, studenten), bv. dreiging voor OV, (regio) Amsterdam, onderwijs, openbare bijeenkomsten, bepaalde (VU) doelgroepen.
2. Is het recente dreigingsbeeld opgevraagd bij het NCTV ("Dreigingsbeeld Terrorisme Nederland", DTN*), zie: <https://www.nctv.nl/>
*) Beleidsimplicaties DTN. *Het Dreigingsbeeld Terrorisme Nederland (DTN) is een globale analyse van de nationale en internationale terroristische dreiging tegen Nederland, en Nederlandse belangen in het buitenland. Het DTN wordt 4 maal per jaar uitgegeven.*
3. Is er verificatie geweest omtrent een vanuit het NCTV binnengekomen dreigingsmelding bij de VU? (algemene nummer NCTV terugbellen tel: 070 751 50 50 (tussen 7.00 en 19.00 uur).
4. Is er proactief getoetst bij politie en AIVD en teruggekoppeld aan CvB en C&M?
5. Geeft het dreigingsbeeld aanleiding om contact op te nemen met het NCTV, bijvoorbeeld aanslag op de categorie 'soft targets'. Zo nee, is aanvullende info NCTV gewenst? *N.B: De VU is een zgn. 'soft target', denk aan winkelcentra, concerten, bioscopen, horeca en treinstations. Informatie is vaak incompleet.*
6. Is er contact met de gemeente (b.v. dossierhouder radicalisering afdeling Openbare Orde en Veiligheid) bij concrete signalen over radicalisering?
7. Is vooraf afgestemd wie vanuit de VU als liaison deelneemt aan het Regionaal Operationeel Team (ROT) van de externe hulpdiensten?
8. Is contact met de lokale driehoek noodzakelijk? (burgemeester, de (hoofd)officier van justitie, de lokale politiechef).
9. Is er contact met UvA, ACTA en AUmc over een aktueel dreigingsbeeld? Met andere HO instellingen?

Inventarisatie

10. Welke (mix van) bijeenkomsten/evenementen worden de komende maanden in de VU gehouden? Ook promoties e.d.. Is er een combinatie van evenementen en vervoersbewegingen aanwezig?
11. Is het aantal en de aard van de zaalreserveringen nagelopen? Zijn er afwijkende patronen? (mn. bepaalde 'risicogroepen').

12. Is er een impact op de onderwijsactiviteiten te verwachten?
13. Welke buitenlandse reizen staan er voor het CvB gepland? (ivm. terugroep).
14. Zijn er bijzondere kwetsbaarheden binnen de VU? (bv. (ver-)bouw en bouwplaatsen, tijdelijke voorzieningen, bijzondere (externe) groepen, conflicterende evenementen, parkeergarages, activiteiten studentenverenigingen etc., open terrein met veel mensen).
15. Is het overzicht van gebouwen aanwezig met de te verwachten bezetting?

Communicatie en maatregelen:

16. Is het SBT/OCT en hoofd beveiliging geïnformeerd? Is er afstemming tussen betrokkenen? Is de SBT ruimte op orde (2B-12)? Is crisisdraaiboek C&M in werking?
17. Heeft de alarmcentrale MBC alle actuele informatie (factsheets, oproepschema)? Zijn bellijsten actueel?
18. Is alle info mbt. factsheets 'dreiging' en 'extreem geweld' actueel?
19. Hebben alle relevante personen (SBT, OCT) NL-alert op eigen smartphone geactiveerd? Whatsapp groep?
20. Is afgesproken/vastgesteld wie de regie heeft over de (externe/interne) communicatie?
21. Is inrichting van een (centraal) informatiepunt (fysiek/digitaal) nodig? Of de voorbereiding daarop?
22. Zijn 'standaard' communicatieberichten klaar indien:
 - Ontruiming grote delen/gehele VU noodzakelijk is;
 - Zo veel mogelijk thuiswerk door medewerkers noodzakelijk is;
 - Bepaalde activiteiten gestopt moeten worden;
 - Een specifieke wijze van communicatie noodzakelijk is (via WhatsApp groepen of centrale sms, mailadressen doelgroepen beschikbaar).
23. Zijn de volgende maatregelen overwogen?
 - Beveiliging informeren/opschalen, actieve monitoring: fysiek/camera's en digitaal;
 - Extra beveiliging bestuursvleugel, CCE, NU-gebouw, grote hal HG/aula/VU-binnenplein, UPC, parkeergarages, afvaldepot, opslag gevaarlijke stoffen, hoge druk gasleiding etc.;
 - Heroverwegen sluitingstijden VU incl. zondag openstelling;
 - VU als opvanglocatie voor derden/ Afstemming Zuid-as;
 - Is overnachting of langdurig verblijf noodzakelijk? Voor zowel intern als extern aanbod. Welke locatie te regelen (foyer aula 1^e ver. HG, Atrium MF)? Welke middelen zijn daarvoor Nodig: extra catering, schoonmaak, beveiliging, logistiek.
 - OV-gebied rond VU (reizen van/betrokkenheid bij medewerkers/studenten, externen);
 - Geplande werkzaamheden door derden beoordelen op risico's voor de VU?;
 - Informeren studentenverenigingen en derden op het terrein: SPAR, Doppio, schoonmaak, catering, OZW-gebouw etc., communicatie omgeving;
 - Zijn contacten gelegd ivm. uitwijkmogelijkheden? RAI, parkeren etc.;
 - Interne communicatie; oproep alertheid? Twitter. Meld- en adviespunt op startscherm PC zetten. Apart telefoonnummer/mailadres voor vragen?

Informatiebronnen:

websites NCTV.nl, Crisis.nl., publicatie 'Handreiking terrorismebestrijding voor bedrijven', NCTV. Om aan de informatievraag te kunnen voldoen, heeft de NCTV diverse crisiscommunicatiemiddelen ontwikkeld: www.crisis.nl, publieksinformatienummer 0800 1351 en de risico- en crisisbarometer. Alle overheden, nationaal, regionaal en lokaal, mogen tijdens een crisis gebruikmaken van deze middelen.

Nagaan van het landelijk dreigingsniveau:

- www.crisis.nl, publieksinformatienummer 0800 1351.

- <https://www.nctv.nl/>
- <https://www.nctv.nl/onderwerpen/dtn>
- <https://www.denkvooruit.nl/risicos/overzicht/een-aanslag>

De *gemeente* Amsterdam is in eerste instantie verantwoordelijk voor het veiligheidsbeleid:

- De politie is het eerste aanspreekpunt voor bedrijven bij een terroristische dreiging of bij verdachte of ongebruikelijke handelingen.
- De gemeente bekijkt terrorismebestrijding doorgaans vanuit het perspectief van het brede veiligheids- en crisisbeheersingsbeleid. Terrorismebestrijding valt daardoor vaak onder de ambtenaar Openbare Orde en Veiligheid of de ambtenaar Rampenbestrijding en/of Bevolkingszorg. De politie kan op locatie komen, de regie overnemen en maatregelen treffen.
- Bedrijven die *melding of aangifte* doen bij de plaatselijke politie van dreigingen, ongebruikelijke handelingen of verdachte objecten, krijgen waarschijnlijk te maken met de *portefeuillehouder Conflict- en Crisisbeheersing* (CCB) van de politie.
- Niet acute situaties: Openbare orde en veiligheid: 020-552 2049 of infovb@amsterdam.nl
- Meld- en adviespunt radicalisering: 020- 552 2684 of adviespuntradicalisering@amsterdam.nl
- Info: <https://www.amsterdam.nl/> .

Concrete dreiging en rol openbaar bestuur:

Wanneer een crisis is veroorzaakt door een terroristische actie of ander ingrijpend strafbaar handelen, bijvoorbeeld een gijzeling, is de *hoofdofficier* degene die leiding geeft aan de behandeling van de crisis tot aan het moment waarop het strafbaar handelen is beëindigd en het herstel van de openbare orde weer centraal komt te staan.

De burgemeester is op grond van zijn verantwoordelijkheid voor de openbare orde primair verantwoordelijk voor de bewaking en beveiliging van objecten en diensten.

Wanneer er echter een concrete dreiging is van een aanslag op een object of dienst op een bepaald tijdstip, ligt de verantwoordelijkheid bij de *hoofdofficier*. Hij is dan degene die een dreigingsinschatting kan laten opstellen, maatregelen kan treffen (bijvoorbeeld de inzet van speciale politie-eenheden) en de betreffende instelling laat informeren. Hij informeert ook de burgemeester. Als bij zo'n concrete dreiging ook maatregelen getroffen moeten worden in het kader van de openbare orde en veiligheid, dan vallen deze onder het gezag van de burgemeester (bijvoorbeeld het plaatsen van een afzetting). De hoofdofficier en de burgemeester stemmen de te treffen maatregelen af in de gezagsdriehoek (h. officier, burgemeester, korpschef).

Bijlage 1. Uitleg nationale dreigingsniveaus en acties VU

<https://www.nctv.nl/onderwerpen/dtn/over-het-dtn-en-het-dreigingsniveau/opbouw-dreigingsniveaus>

Hieronder zijn bij elk van de dreigingsniveaus enkele elementen opgesomd die, als zij aan de orde zijn, richting geven bij het bepalen van het dreigingsniveau.

Dreigingsniveaus

1

De terroristische dreiging in Nederland is minimaal

Het is niet waarschijnlijk dat in Nederland een terroristische aanslag plaatsvindt.

- We hebben geen aanwijzingen dat zich in Nederland personen bevinden die een terroristische dreiging vormen.
- We hebben geen aanwijzingen dat Nederland in beeld is bij terroristen in het buitenland.

2

De terroristische dreiging in Nederland is beperkt

Er bestaat een kleine kans op een terroristische aanslag in Nederland.

- Er is sprake van radicalisering waarvan op termijn een dreiging kan uitgaan.
- Terroristen hebben de intentie aanslagen te plegen in Europa, maar treffen daartoe geen concrete voorbereidingen.

3

De terroristische dreiging in Nederland is aanzienlijk

Een terroristische aanslag in Nederland is voorstelbaar.

- Er zijn in Nederland personen en groepen die sterk radicaliseren en een dreiging vormen.
- We hebben geen aanwijzingen dat terroristen een aanslag in Nederland voorbereiden, maar het is wel voorstelbaar.
- Terroristen plegen of plannen aanslagen in Europa.

4

De terroristische dreiging in Nederland is substantieel

De kans op een terroristische aanslag in Nederland is reëel.

- Terroristen zien Nederland als een doelwit.
- Terroristen plegen aanslagen in omliggende landen.
- Mogelijk zijn er aanwijzingen dat terroristen een aanslag op Nederland voorbereiden.

5

De terroristische dreiging in Nederland is kritiek

Een terroristische aanslag in Nederland is op handen.

- We hebben concrete aanwijzingen dat terroristen op het punt staan een aanslag in Nederland te plegen.
- Er heeft een aanslag in Nederland plaatsgevonden.
- Er is een kans op een vervolgaanslag in Nederland.

VU actie CIV niveaus 3 en 4:

Bij de **niveaus 3 en 4** zijn er nog onzekerheden. Een aanslag in Nederland kan worden voorbereid. Uit de context kan worden opgemaakt of de VU (c.q. Onderwijs, Amsterdam, etc.) mogelijk doelwit kan zijn. Via het NCTV kunnen signalen aan de VU worden afgegeven.

- Context van dreigingsniveau bekijken, website NCTV);
- Standaard agendapunt en regie in CIV: ontwikkeling blijven volgen;
- Extra aandacht voor meld- en adviespunt (alertheid);
- Checklist 'omgaan met dreiging' factsheet nalopen en afwegen maatregelen, ook als voorbereiding op niveau 5.

Dreigingsniveau 5 wordt in Nederland van kracht als een aanslag in Nederland op handen is of mogelijk een vervolgaanslag.

VU actie SBT (niveau 5):

- Idem niveau 3/4 + de hierna genoemde activiteiten;
- SBT 'stand-by', periodiek bijeen; factsheet 'extreem geweld' activeren;
- Instructies voor (leidinggevend van) MBC-CCE;

- NL alert activeren op smartphones OCT en SBT, monitoren crisis.nl / 0800-1351 (publieksinfolnummer); Nationaal CrisisCentrum (NCC)
<https://www.rijksoverheid.nl/contact/contactgids/nationaal-crisiscentrum-ncc>
- Zorgvuldig omgaan met (grote) bijeenkomsten, heroverwegen daarvan;
- Contact leggen met gem. Amsterdam/politie (info uitwisseling), dreigingskader vaststellen;
- Checklist 'omgaan met dreiging' factsheet nalopen en concrete actiepunten vaststellen.

Opties op basis van verkregen info:

- Beveiliging opschalen, actieve/gerichte monitoring: fysiek/camera's en digitaal;
- OV-gebied rond VU (reizen van/betrokkenheid bij medewerkers/studenten) en effect op de VU (opvang, reizigersbeperkingen, colleges, bijeenkomsten etc.);
- VU als opvanglocatie voor derden / Afstemming met Zuid-as;
- Interne communicatie; oproep alertheid? Meld- en adviespunt op startscherm PC.

Uit de *context* van de informatie worden de te nemen stappen en (interne) communicatie besproken, waar nodig in overleg met bv. gemeente, overige universiteiten, AUMc, UvA, politie, e.d..

Bijlage 2, Checklist vanuit gemeente Amsterdam

Gemeente Amsterdam

Datum 4 juli 2018

Checklist terrorisme scenario's

Scenario	Denk aan:
Dreiging op uw onderneming	<ul style="list-style-type: none">• Noteer zo exact mogelijk alle gegevens over de melding van de dreiging;• Meld een dreiging bij politie via 112 (de politie analyseert en duidt de dreiging);• Maak een analyse van de situatie (in uw crisisteam);• Hou bij het voorbereiden van maatregelen en communicatie de analyse van de dreiging in gedachten;• Voorkom het nemen van overhaaste en ondoordachte maatregelen en besluiten;• Benader geen verdachte objecten;• Maak een inventarisatie van de aanwezigen in uw onderneming;• Denk na over interne en externe communicatie.
Dreiging op andere ondernemingen of andere locatie in de buurt, de stad of Nederland.	<ul style="list-style-type: none">• Inventariseer de feiten;• Heeft u vragen, neem contact op met de politie (wijkagent) of de overheid;• Maak een analyse (in uw crisisteam) van de impact die de dreiging mogelijk kan hebben op uw werknemers en bezoekers;• Denk na over communicatie (intern en extern);• Als u communiceert, geef dan een handelingsperspectief;• Voorkom het nemen van overhaaste en ondoordachte maatregelen en besluiten.
Aanslag in uw directe omgeving	<ul style="list-style-type: none">• Bel zo snel als mogelijk met 112;• Vluchten of verstoppen;• Hou rekening met snelle interventie-eenheden op of nabij uw onderneming;• Stem communicatie direct na de aanslag zo veel mogelijk af met de overheid;• Maak een inventarisatie van de aanwezigen in uw onderneming;• Wijs een contactpersoon/liaison aan voor de overheid.
Aanslag op andere locatie in de stad of Nederland.	<ul style="list-style-type: none">• Inventariseer de feiten;• Heeft u vragen, neem contact op met de politie (wijkagent) of de overheid;• Maak een analyse van de impact en behoeften die de aanslag mogelijk kan hebben op uw onderneming;• Denk na over communicatie (intern en extern);• Als u communiceert, geef dan een handelingsperspectief;• Voorkom het nemen van overhaaste en ondoordachte maatregelen en besluiten.
Algemene tips in de voorbereiding	<ul style="list-style-type: none">• Een ontruimingsplan (naar huis, op straat of naar de burelen);• Een schuilplan in uw locatie;• Instellen crisisteam;• Inventariseren van cruciale besluiten tijdens de verschillende scenario's, inclusief wie de besluiten mag nemen;• Communicatie: intern en extern;• Praktische hulpmiddelen op orde hebben (zie maatregelen);• Afspraken maken met de omgeving en wijkagent om samen te werken;• Organiseer een crisisoefening.

Bijlage 3, WAVR instrument dreigingscasuïstiek

Instrument beoordeling werkplek en campus gerichte dreigingscasuïstiek

Zorgwekkend en ongewenst gedrag bij medewerkers en studenten komt voor. Het zorgwekkende gedrag kan ook afkomstig zijn van klanten, voormalige werknemers of onbekenden die de organisatie trachten te benadelen. Er zijn tal van gedragingen die we kunnen betitelen als 'ongewenst of zorgwekkend'. Voorbeelden van dergelijk gedrag varieert van (interpersoonlijke) agressie, seksuele intimidatie, stalking, dreigementen tot aan beschadiging van eigendommen en het opzettelijk verspillen/vernielen van VU eigendommen. Met de WAVR is het mogelijk om dit gedrag vast te stellen, te onderzoeken en te managen.

Methode om de ernst van een dreiging in te kunnen schatten d.m.v. 'gestructureerde professional judgement': *The WAVR-21 – Workplace Assessment of Violence Risk – is a 21-item coded instrument for the structured assessment of workplace and campus targeted violence risk. It is also applicable to students, 18 years of age or older in campus contexts.* Bron: <http://www.wavr21.com/>

The WAVR-21 Items: Definitions, Explanations, and Coding Criteria

1. Motives for Violence
2. Homicidal Ideas, Violent Preoccupations or Identifications
3. Threatening Communications or Expressed Intent
4. Weapons Skill and/or Access
5. Pre-attack Planning and Preparation
6. Stalking or Menacing Behavior
7. Current Job or Academic Problems
8. Extreme Job or Academic Attachment
9. Loss, Personal Stressors and Negative Coping
10. Entitlement and Other Negative Traits
11. Lack of Conscience and Irresponsibility
12. Anger Problems
13. Suicidality and/or Depressive Mood
14. Irrationally Suspicious or Bizarre Beliefs
15. Substance Abuse and/or Dependence
16. Increasing Isolation
17. History of Violence, Criminality, and/or Conflict
18. Domestic/Intimate Partner Violence
19. Situational and Organizational Contributors to Violence
20. Stabilizers and Buffers Against Violence
21. Organizational Impact of Real or Perceived Threats