Tussen mogelijkheid en realiteit

Een empirisch onderzoek naar de inzet van drones door terroristen, eenlingen, criminelen en statelijke actoren in het Westen tussen 2010 - 2025

Stijn Willem van 't Land

Universiteit Leiden
Institute of Security and Global Affairs

Contents

Managementsamenvatting **3**
Introductie, probleemstelling en afbakening **4**
Dronegebruik door kwaadwillende actoren tot nu toe: wie, wat, en hoe? **6**
Achtergrond 6
Typen drones die gebruikt worden door kwaadwillende actoren 6
Deel I: Theorie **10**
Bevorderende en remmende factoren voor innovatie door dreigingsactoren 10
Endogene factoren *10*
Exogene factoren *10*
Gemengde factoren *11*
De aantrekkingskracht van drones 11
Relatief voor- en nadeel *11*
Compatibiliteit *13*
Complexiteit *13*
Beproefbaarheid *14*
Observeerbaarheid *15*
Resumerend *15*
Leer- en innovatieroutes voor dreigingsactoren 17
Deel II: Empirische studie **19**
Methode 19
Inclusie- en exclusiecriteria 19
Bronnen 20
Resultaten 20
Discussie 24
Beperkingen 28
Praktijkaanbevelingen 28
Verder onderzoek 29
Conclusie **31**
Appendix A: Codeboek voor empirische studie **32**
Bibliografie **33**

Managementsamenvatting

Het doel van deze studie was om systematisch in kaart te brengen hoe kwaadwillende actoren die relevant zijn voor het stelsel bewaken en beveiligen sinds 2010 drones hebben gebruikt (of gepoogd te gebruiken) voor het plegen van aanslagen in Westerse landen. Ook is een theoretisch afwegingskader ontwikkeld dat kan helpen te duiden waarom de inzet van drones door dreigingsactoren – ondanks de zichtbaarheid en beschikbaarheid van drones – vooralsnog relatief beperkt blijft. Het rapport combineert dit theoretisch afwegingskader met een open bronnenonderzoek van incidenten in de periode 2010 tot en met 2025. Hieronder een overzicht van de meest relevante bevindingen.

Kernbevindingen

De omvang van aanslagen met drones of plannen daartoe is beperkt, al is er een recente toename: er werden 34 incidenten geïdentificeerd tussen 2010 en 2025. In 2024 en 2025 werden acht incidenten per jaar geregistreerd, een duidelijke en aanzienlijke stijging ten opzichte van eerdere jaren.

Drones fungeren vooral als (beoogd) aanslagmiddel, minder als middel voor voorverkenning: bij 25 van de 34 incidenten was het doel de drone (met payload) als direct aanslagmiddel te gebruiken.

Commerciële en zelfgemaakte drones zijn populair: waar het viel te herleiden, werden bij de meeste incidenten commerciële drones gebruikt, gevolgd door zelfgemaakte drones. Militaire en industriele drones zijn minder populair.

Hard targets zijn vaak doelwit: waar het doel van het gebruik van de drone voor de aanslag(poging) kon worden vastgesteld, was dit in alle gevallen gerelateerd aan het overkomen van beveiligingsmaatregelen rondom hard targets.

Veel aanslagplannen met drones stranden voor uitvoering of mislukken: meer dan de helft van de incidenten uit de dataset betreft aanslagplannen die niet ten uitvoer kwamen. Slechts twaalf incidenten kwamen tot uitvoering, en bij vier van deze incidenten bereikte de aanslagplegers het uiteindelijke doel van de inzet van de drone niet.

Aanslagplannen met een drone zijn vaak wel vergevorderd: bij 65% van de incidenten waarbij zeker was dat de drone als aanslagmiddel was bedoeld, werden explosieven of precursoren daarvoor aangetroffen.

De verijdeling van incidenten met drones verloopt vooral via intelligence: bij alle incidenten die voorkomen werden was dit het gevolg van vroegtijdige detectie en interventie door de veiligheidsdiensten, niet als gevolg counterdrone-technologie.

Attributie is vaak mogelijk: bij 82% van de incidenten slaagden autoriteiten erin om het incident aan één of meerdere daders toe te schrijven.

Aanslagen met drones zijn populair onder eenlingen en terroristische organisaties: meer dan de helft van de incidenten zijn toe te schrijven aan eenlingen en dyades, gevolgd door terroristische groepen. Criminele samenwerkingsverbanden en statelijke actoren zijn nauwelijks betrokken bij incidenten.

Jihadisten zijn de voornaamste actoren achter aanslag(plannen) met drones: binnen de groep eenlingen, dyades en terroristische organisaties hing een substantieel deel van de incidenten samen met jihadistisch gedachtegoed. Een groot deel hiervan was geïnspireerd door Islamitische Staat (IS).

Online netwerken spelen een belangrijke rol: veel daders bespreken hun aanslagplannen online, of consumeren of delen (technische) instructies en handleidingen over drones in online netwerken.

Introductie, probleemstelling en afbakening

De proliferatie van drones heeft er de afgelopen vijftien jaar voor gezorgd dat drones niet meer weg te denken zijn uit de samenleving. Ze worden volop gebruikt door hobbyisten en door commerciële partijen. Ook zijn drones essentieel in het veiligheidsdomein: ze worden door politie en defensie gebruikt om doelwitten te bewaken of juist aan te kunnen vallen. Gelet op de mogelijkheid van het inzetten van drones als wapen bestaan er groeiende zorgen over de inzet van drones door kwaadwillende actoren zoals terroristische groeperingen, gewelddadige eenlingen, criminele samenwerkingsverbanden en vijandige statelijke actoren.

De laatste jaren waarschuwen experts specifiek voor de inzet van drones door terroristen of criminelen om aanslagen te plegen op personen, grootschalige evenementen of kritieke infrastructuur in Westerse landen (Dalton, 2025; Damiani & Jasper, 2024; Rivera et al., 2025). Gevreesd wordt dat deze actoren leren van ervaringen elders, in het bijzonder het slagveld in Oekraïne, en in het Midden-Oosten en West-Afrika, waar terreurgroepen drones gebruiken om aanslagen te plegen en aanvallen te coördineren. Ook wordt er regelmatig verwezen naar Mexico, waar drugskartels drones inzetten voor het uitvoeren van gerichte aanslagen op rivalen, de politie en defensie (Damiani & Jasper, 2024; Veilleux-Lepage & Archambault, 2022).

In Nederland klinken er ook zorgen. "Plegen Amsterdamse criminelen straks liquidaties met drones uit Oekraïne?" kopte het Parool in januari 2026 (Laumans & Vugts, 2026). Naar aanleiding van een verijdeld aanslagplan met een drone op de Belgische premier Bart de Wever en Nederlandse politicus Geert Wilders werden in november 2025 Kamervragen gesteld over mogelijke terroristische aanslagen met drones in Nederland. De indiener van de Kamervragen vroeg zich onder meer af of er signalen zijn dat dreigingsactoren in Nederland drones willen inzetten voor aanslagen en in hoeverre de Nederlandse autoriteiten deze ontwikkelingen actief monitoren (Van Oosten, 2025). De reactie van de minister van Justitie en Veiligheid was nuchter: de omvang van drone-aanslagen in het Europa en het Westen is vrijwel nihil; een conclusie die de Nationaal Coördinator Terrorismebestrijding- en Veiligheid in juni 2024 ook trok (Nationaal Coördinator Terrorismebestrijding- en Veiligheid, 2024).

Hoewel het schrikbeeld van 'de drone als wapen' de gemoederen dus bezighoudt, heerst tegelijkertijd de opvatting dat er in het Westen nauwelijks incidenten met drones zijn. In het licht van deze paradox is het opvallend dat er tot op heden weinig systematisch onderzoek is gedaan naar het daadwerkelijke gebruik van drones door kwaadwillende actoren in Westerse landen. Bestaand onderzoek richt zich voornamelijk op de andere eerdergenoemde regio's (Haugstvedt, 2024; Krame & and Davies, 2023; Veilleux-Lepage & Archambault, 2022) of is verkennend, conceptueel en tamelijk speculatief (en soms zelfs wat alarmistisch) van aard (Bouhlaoui, 2025; Damiani & Jasper, 2024).

Tegelijkertijd is de aanname dat de ervaring met drones uit andere contexten zullen worden overgenomen door kwaadwillende actoren in het Westen niet geheel ongegrond. Er zijn concrete voorbeelden van kwaadwillende actoren in het Westen, waaronder criminele groepen, die gebruik maken van drones. Denk bijvoorbeeld aan het smokkelen van drugs of telefoons in penitentiaire inrichtingen (Dienst Justitiële Inrichtingen, 2022). Ook wordt het mogelijke gebruik van drones voor aanslagen in het Westen breed uitgemeten in propaganda van verschillende rechtsextremistische en jihadistische terroristische groeperingen (Nationaal Coördinator Terrorismebestrijding- en Veiligheid, 2024).

Kortom, de dreiging is voorstelbaar. Maar ondanks de ogenschijnlijke beschikbaarheid van middelen, kennis en inspiratiebronnen voor dreigingsactoren, lijken drones in het Westen tot nu toe slechts in beperkte mate daadwerkelijk te worden ingezet voor het plegen van aanslagen, of ter ondersteuning daarvan. Dit roept vragen op over de aannames die ten grondslag liggen aan het schrikbeeld dat steeds dominanter lijkt. Op welke empirie is de huidige dreigingsinschatting ten aanzien van dit fenomeen gebaseerd? Wat is de aard en omvang van aanslagen met drones door kwaadwillende actoren in het Westen – of pogingen daartoe – werkelijk? En welke factoren moeten worden meegewogen om het gat tussen mogelijkheid en de realiteit van aanslagen met drones door kwaadwillende actoren te verklaren?

In dit rapport is in twee delen gepoogd deze vragen te onderzoeken. In deel I van het rapport is verkend welke factoren de adoptie – dan wel de non-adoptie – van drones door kwaadwillende actoren verklaren. Daarmee is beoogd bij te dragen aan een breder theoretisch-analytisch kader voor dreigingsinschatting op fenomeenniveau en de monitoring van incidenten, met specifieke aandacht voor het gebruik van drones door kwaadwillende actoren die te relateren zijn aan de dreigingsfenomenen die relevant zijn voor het stelsel bewaken en beveiligen, te weten: georganiseerde criminaliteit, terrorisme, statelijke actoren en geradicaliseerde eenlingen (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2023). Hiertoe is gebruik gemaakt van literatuur over de implementatie en adoptie van innovaties en recente rapporten en studies die inzicht bieden in het gebruik van drones door kwaadwillende actoren. Daarnaast is in deel II van het rapport een systematische empirische inventarisatie uitgevoerd van de daadwerkelijke inzet van drones ten behoeve van (het voorbereiden van) het plegen van aanslagen door deze actoren. Deze inventarisatie brengt de aard en omvang van het gebruik van drones door dreigingsactoren in Westerse landen in de periode 2010 tot en met 2025 in kaart, evenals (onder andere) operationele details over de geïdentificeerde aanslag(pogingen) en sociaaldemografische data over de daders of verdachten.

De studie is afgebakend tot incidenten met drones waarbij deze zijn gebruikt bij het plegen van een aanslag op een persoon of object, of ter ondersteuning van een aanslag. In de context van afbakening moet ook benadrukt worden dat het zwaartepunt van deze studie ligt op gebruik van drones door niet-statelijke actoren. Hoewel drones in andere contexten veelvuldig door statelijke actoren worden ingezet, is het gebruik van drones door staten voor het plegen of ondersteunen van aanslagen op personen of objecten in Westerse landen in de literatuur beperkt beschreven. Bestaande publicaties richten zich voornamelijk op militaire inzet in conflictgebieden en *grey zone*-activiteiten, en minder op geweldstoepassing die relevant is voor het domein van bewaken en beveiligen; aanslagen op personen of objecten. Bovendien gelden voor statelijke actoren – vanwege hun grote capaciteit, hoge mate van organisatie, diplomatieke overwegingen en geduld – mogelijk wezenlijk andere afwegingen bij de inzet van drones voor het plegen van een aanslag dan voor niet-statelijke actoren. Hierdoor is het in deze studie ontwikkelde afwegingskader slechts in beperkte mate op statelijke actoren gebaseerd en daarom waarschijnlijk ook minder goed toepasbaar. Empirisch wordt deze afbakening ondersteund door het feit dat niet-statelijke actoren binnen de onderzochte periode verantwoordelijk zijn voor 33 van de 34 incidenten.

De studie laat zien dat het gebruik van drones door kwaadwillende actoren in Westerse landen tot dusver beperkt is, maar de afgelopen jaren wel is toegenomen. Het merendeel van de geïdentificeerde incidenten betreft verijdelde aanslagplannen van eenlingen en dyades, vaak geïnspireerd door jihadistisch gedachtegoed. De inzet van drones ten behoeve van een aanslag lijkt bovendien complex. Op basis van de data lijkt de succesvolle uitvoer van een aanslag vooral te worden belemmerd door vroegtijdige detectie en interventie door de veiligheidsdiensten. Ook lijkt het verkrijgen van toegang tot een explosief om met de drone te gebruiken een belangrijke bottleneck voor het uitvoeren van een aanslag met een drone. Uit de data blijkt ten slotte dat drones primair worden overwogen om beveiligde doelwitten, zogenaamde *hard targets*, te bereiken.

Om het fenomeen van dronegebruik door kwaadwillende actoren in context te plaatsen, wordt in het volgende hoofdstuk eerst een overzicht gegeven van de bestaande literatuur over de inzet van drones door kwaadwillende actoren. Deze literatuurstudie biedt inzicht in de ontwikkeling, trends, aard en toepassingen van dronegebruik door deze actoren tot op heden en vormt daarmee de basis voor het theoretisch kader en de empirische studie.

Het gebruik van drones door kwaadwillende actoren in Westerse landen is beperkt, maar is de afgelopen jaren wel toegenomen.

Dronegebruik door kwaadwillende actoren tot nu toe: wie, wat, en hoe?

Achtergrond

Het gebruik van drones als onderdeel van oorlogen is geen nieuw fenomeen. Militaire dronetechnologie gaat terug tot de Vietnamoorlog. De inzet van drones door terroristen, eenlingen en criminelen is echter een meer recent fenomeen. Rond de millenniumwisseling experimenteerden een aantal terroristische groeperingen met het inzetten van drones. De Tamil Tijgers in Sri Lanka, Hamas in Gaza en Hezbollah in Libanon zochten sinds de vroege jaren 2000 naar manieren om drones in te zetten voor het plegen van aanslagen (Doctor, 2025; Rossiter, 2018; Veilleux-Lepage & Archambault, 2022). Deze vroege experimenten met drones waren sterk afhankelijk van de eigen ontwikkeling of productie van drones, of van steun van statelijke actoren, zoals bijvoorbeeld Iran. Grootschaliger gebruik van drones door dreigingsactoren kwam daarom pas vanaf het midden van de jaren 2010 op gang, parallel aan de opkomst van de markt voor commerciële drones (Doctor, 2025).

In de literatuur gelden vooral Islamitische Staat in Irak en Syrië (ISIS) en verschillende Mexicaanse kartels – in het bijzonder het CJNG-kartel (Jaliscokartel-Nieuwe Generatie) – als vroege gebruikers van commerciële drones (Bouhlaoui, 2025; Bunker et al., 2020; Doctor, 2025; Krame & and Davies, 2023). In Mexico begonnen drugskartels rond 2012 met grootschalig dronegebruik voor smokkel van contrabande over de grens met de Verenigde Staten. In april 2019 werden drones voor het eerst door de kartels gebruikt om inlichtingen over grenspatrouilles te verzamelen om mensensmokkel te faciliteren. Vanaf 2020 vonden de eerste incidenten en aanslagen met explosieven plaats. Inmiddels is dronegebruik wijdverbreid onder verschillende Mexicaanse kartels (Bunker et al., 2020; Krame & and Davies, 2023; Toledano, 2024). Koerdische strijders in Syrië en Irak rapporteerden vanaf 2015 incidenten met drones in hun strijd tegen ISIS. Hierbij werden drones met explosieven door ISIS gebruikt om Koerdische troepen uit te schakelen. Vanaf 2016 richtte ISIS een eigen drone-eenheid op, en vanaf 2017 schaalde de terreurgroep het gebruik van drones sterk op, onder meer tijdens de strijd om Raqqa en Mosoel (Doctor, 2025; Dulligan et al., 2025; Veilleux-Lepage & Archambault, 2022).

Volgens Doctor (2025) is er de afgelopen jaren sprake van een gefaseerde, wereldwijde diffusie van dronegebruik door dreigingsactoren. Na de vroege experimenten door ISIS en de kartels volgde een tweede golf gebruikers, waaronder bijvoorbeeld de rebellen in Myanmar en de Taliban in Afghanistan. Data van Haugstvedt (2024) laten rond 2019 een exponentiële toename te zien in het succesvolle gebruik van drones voor aanslagen wereldwijd. In de afgelopen jaren is de groep gebruikers verder uitgebreid met onder meer Al-Qaeda in het Arabisch Schiereiland (AQAP), de FARC in Colombia, Al-Shabaab, Islamitische Staat in Mozambique (ISMP), Hayat Tahrir al-Sham (HTS) en Islamitische Staat in West-Afrika (ISWAP) (Doctor, 2025; Haugstvedt, 2024).

Er is de afgelopen jaren sprake van een gefaseerde, wereldwijde diffusie van dronegebruik door dreigingsactoren.

Typen drones die gebruikt worden door kwaadwillende actoren

Dreigingsactoren kunnen van vier typen drones gebruik maken: *militaire*, *industriële*, *commerciële* en *zelfgemaakte* drones (Doctor, 2025). Militaire drones zijn door statelijke actoren of defensieproducenten voor militaire doeleinden ontwikkeld. Zoals eerder benoemd is dit type drone nauwelijks beschikbaar voor dreigingsactoren, tenzij zij steun van een statelijke actor ontvangen (of zelf een statelijke actor zijn), omdat de ontwikkeling ervan gecompliceerd is en veel kennis en middelen vereist (Lubrano, 2023).

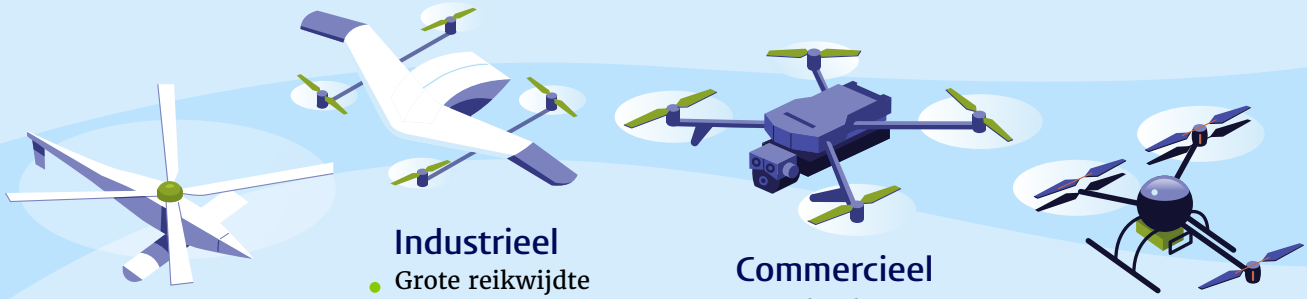
Industriële drones zijn ontworpen voor toepassingen in sectoren als land- of mijnbouw en kenmerken zich vanwege hun industriële doeleinden door een grotere actieradius en payloadcapaciteit dan commerciële

drones. Commerciële drones zijn kant en klare modellen die vrij verkrijgbaar zijn voor hobbyisten, zoals de populaire modellen van DJI. Commerciële modellen die veel gebruikt worden door dreigingsactoren zijn onder andere de DJI Phantom en -Mavic series, 3DR-modellen en FPV-drones zoals de X8 Skyhunter en Skywalker modellen (Bouhlaoui, 2025; Dulligan et al., 2025). Zowel industriële als commerciële drones vereisen doorgaans aanpassingen om explosieven te kunnen dragen en af te leveren, bijvoorbeeld door het 3D-printen van een speciaal aflevermechanisme voor een payload. Ten slotte bestaan er zelfgemaakte drones, welke geheel of gedeeltelijk zelf zijn ontworpen of replica's zijn van andere (militaire) drones. HTS in Syrië bouwt bijvoorbeeld drones die zijn afgeleid van buitgemaakte militaire Russische en Iraanse modellen (Dass, 2024).

Ook kan er onderscheid worden gemaakt tussen *fixed-wing*- en *rotary-wing* modellen: *fixed-wing* drones zijn drones met vleugels die horizontaal opstijgen en deze hebben doorgaans een groter bereik en hogere snelheid, terwijl *rotary-wing* drones – de helikoptermodellen die verticaal opstijgen – beter manoeuvreerbaar zijn en kunnen stilhangen op één plek. Militaire, industriële, commerciële en zelfgemaakte drones zijn allen beschikbaar als zowel *fixed-wing*- als *rotary-wing* modellen, afhankelijk van de specifieke toepassing van de drone.

Tabel 1: Typen drones die gebruikt worden door dreigingsactoren, en relevante karakteristieken

Typen drones die gebruikt worden door dreigingsactoren



Militair
- Geproduceerd voor militaire doeleinden
- Door statelijke actor of defensieproducenten
- Moeilijk te bemachtigen

Industrieel
- Grote reikwijdte
- Grote payload-capaciteit
- (Vaak) aanpassingen nodig

Commercieel
- Overal te koop
- Wendbaar
- Kleine reikwijdte
- Lage payload-capaciteit
- (Vaak) aanpassingen nodig

Zelfgemaakt
- Naar eigen behoeften te bouwen
- Moeilijk onderdelen te bemachtigen
- Moeilijk te bouwen

Vliegtuigmodel
- Relatief grote reikwijdte
- Hoge snelheid
- Efficiënt (in batterij- of brandstofverbruik)

Helikoptermodel
- Relatief kleine reikwijdte
- Lagere snelheid
- Relatief inefficiënt
- Kunnen op één plek blijven hangen
- Makkelijk te manouvreren

Toepassingen van drones door kwaadwillende actoren

De drone is dus geen eenduidig object: typen verschillen sterk in beschikbaarheid, payloadcapaciteit, aanpasbaarheid en operationele voordelen en beperkingen. Net zoals de variëteit in typen drones, is er ook veel variatie in hoe drones in de praktijk door dreigingsactoren worden benut. Veilleux-Lepage en Archambault (2022) ontwikkelden een uitgebreide typologie van drone-gebruik door terroristen. Deze typologie sluit ook goed aan op het soort gebruik dat er in de literatuur wordt toegekend aan andere dreigingsactoren, zoals bijvoorbeeld de kartels in Mexico. Om die reden wordt het model van Veillieux-Lepage en Archambault – met een kleine aanpassing – in deze studie direct overgenomen, met uitzondering van enkele toepassingen uit het model die niet relevant zijn voor het taakveld van bewaken en beveiligen.

De drone is geen eenduidig object: typen verschillen sterk in beschikbaarheid, payloadcapaciteit, aanpasbaarheid en operationële voordelen en beperkingen.

Tabel 2: Typologie van toepassingen van drones door dreigingsactoren (Veilleux-Lepage & Archambault, 2022)

ISR	Communicatie	Disruptie en dreiging	Aanslag
Voorverkenning Real-time intelligence Signals intelligence (SIGINT)	Direct communicatiemiddel Propagandaproductie	Intimidatie Bedreiging Verstoring	Kamikaze (*Pilot-to-Target*) Payload laten vallen Vuurwapen op drone Logistiek hulpmiddel

Allereerst kunnen drones worden gebruikt voor zogenaamde *intelligence, surveillance & reconaissance*-toepassingen (ISR) (Doctor, 2025; Dulligan et al., 2025). Dit omvat voorverkenning van doelwitten, het in kaart brengen van beveiligingsmaatregelen, of het leveren van real-time inlichtingen tijdens de uitvoering van een aanslag. In Mexico worden drones op deze manier gebruikt door kartels om grondoperaties door hun 'infanteristen' of grondtroepen te ondersteunen (Bunker & Sullivan, 2021b). In theorie kunnen drones ook worden gebruikt voor SIGINT (*signals intelligence*), bijvoorbeeld voor het onderscheppen van wifi- of bluetoothsignalen rondom beveiligde locaties, of het opzetten van nepnetwerken rondom een woon- of werkomgeving, om zo gevoelige data van een doelwit buit te maken (Veilleux-Lepage & Archambault, 2022).

Ten tweede kunnen drones worden ingezet voor communicatiedoeleinden; bijvoorbeeld om boodschappen te verspreiden, via het strooien van pamfletten of via luidsprekers die zijn bevestigd aan een drone (Veilleux-Lepage & Archambault, 2022). Relevanter voor bewaken en beveiligen is echter het mogelijke gebruik van drones voor de productie van propaganda. Dreigingsactoren, waaronder terroristische groeperingen en Mexicaanse kartels, gebruiken drones om beelden van aanslagen of aanvallen te produceren en te verspreiden – om slagkracht uit te stralen, anderen te inspireren om een aanslag met een drone te plegen, of psychologische impact op burgers, overheden of hun tegenstanders uit te oefenen (Doctor, 2025; Krame & and Davies, 2023).

Ten derde kunnen drones worden gebruikt voor smokkel- en logistieke doeleinden. Drones kunnen beveiligingsmaatregelen omzeilen en worden ingezet voor het vervoeren van wapens of andere goederen. Een bekend voorbeeld in Nederland is het gebruik van drones om smokkelwaar in penitentiaire inrichtingen te brengen (Dienst Justitiële Inrichtingen, 2022). Zo is het ook voorstelbaar dat drones aanslagplegers logistiek kunnen ondersteunen; door hen tijdens de voorbereiding of uitvoering van een aanslag van middelen te voorzien, bijvoorbeeld op moeilijk bereikbare locaties (Veilleux-Lepage & Archambault, 2022).

Ten vierde kunnen drones – zonder directe geweldsintentie – als disruptie- of dreigingsmiddel worden ingezet. Ze kunnen veiligheidsdiensten afleiden of verstoren en op die manier een aanslagpoging ondersteunen. Bij een ontzetting van een gijzeling door de FBI in 2018, werd een observatieteam van de FBI bestookt met drones zonder payload, om het team zo 'blind' te maken (Police1, 2018). Ook kan de aanwezigheid van drones op zichzelf al onrust veroorzaken, zonder dat er daadwerkelijk op een doelwit wordt afgevlogen – zoals bleek bij incidenten rond militaire bases in Europa eind 2025 (Boffey & Bryant, 2025). Drones kunnen daarnaast worden ingezet om te dreigen, bijvoorbeeld door hun aanwezigheid te combineren met het afleveren van een dreigement. Een voorbeeld hiervan is een actie door een onbekend kartel in Mexico, waarbij twee drones bij de voordeur van een bekende veiligheidsambtenaar in Baja California werd afgeleverd. Aan de ene drone waren twee onklaar gemaakte explosieven bevestigd, en aan de andere een foto van het gezin van de ambtenaar. Op deze wijze wordt dreiging gecommuniceerd via het impliciete signaal dat een aanval met een drone mogelijk is, maar (vooralsnog) besloten is de aanslag niet te plegen (Krame & and Davies, 2023).

Ten slotte kunnen drones als daadwerkelijk aanslagmiddel worden ingezet. Grofweg zijn er drie praktische toepassingen om drones als direct aanslagmiddel in te zetten. Ze kunnen fungeren als kamikazedrone – de zogenaamde *Pilot-to-Target* toepassing; ze kunnen worden gebruikt om explosieven af te leveren boven een doelwit; of – in uitzonderlijke gevallen – kunnen drones worden uitgerust met een vuurwapen om een doelwit te beschieten (Veilleux-Lepage & Archambault, 2022). De laatste toepassing wordt op het slagveld in Oekraïne al ingezet, maar het gebruik van deze toepassing door dreigingsactoren wordt in de huidige (empirische) literatuur nog niet gerapporteerd.

Dreigingsactoren kunnen drones inzetten voor communicatiedoeleinden, als middel voor voorverkenning en het vergaren van intelligence, als middel om mee te dreigen of als middel om een aanslag mee te plegen.

Deel I: Theorie

Bevorderende en remmende factoren voor innovatie door dreigingsactoren

Voordat de empirische bevindingen van de huidige studie worden besproken, wordt in de volgende sectie eerst uitgebreid de literatuur over innovaties behandeld, om vanuit theoretisch oogpunt te beredeneren welke factoren mogelijk verklaren hoe een dreigingsactor tot de beslissing komt om een drone wel of niet in te zetten. De beschikbaarheid van een nieuwe technologie en kennis daarover betekent immers niet automatisch dat een actor ook daadwerkelijk tot de inzet van die nieuwe technologie (zoals drones) overgaat. Adoptie is het resultaat van een wisselwerking en combinatie van actor-gerelateerde factoren, omgevingscondities die het gebruik ervan wel of niet permitteren, en kenmerken van de technologie zelf (Lubrano, 2023; Moore & McKenna, 2001; Rogers, 1983). Lubrano (2023) ontwikkelde een raamwerk van factoren die innovatie door terroristische organisaties bepalen en onderscheidt hierbij endogene, exogene en gemengde factoren. In deze studie wordt dit raamwerk niet alleen toegepast, maar ook verbreed door het te betrekken op andere niet-statelijke dreigingsactoren en aan te vullen met literatuur over dronegebruik door deze actoren.

Endogene factoren

Endogene factoren hangen volledig samen met de actor zelf. Allereerst spelen pragmatische factoren een rol bij de keuze om een technologie wel of niet te adopteren: (1) beschikbare middelen bepalen in hoge mate of een actor kan experimenteren met nieuwe technologie. Actoren met weinig middelen kiezen logischerwijs vaker voor goedkope en laagdrempelige aanvalsmethoden en -middelen, terwijl grotere organisaties meer ruimte hebben om te oefenen, en aan *trial-and-error* te doen met nieuwe technologieën en nieuwe modus operandi. Ook (2) de organisatiestructuur van een actor – of de persoonlijkheden van individuen binnen een organisatie – kunnen innovatie remmen of bevorderen. Sommige dreigingsactoren hebben eigen, specialistische innovatie-afdelingen. De kartels in Mexico richtten bijvoorbeeld gespecialiseerde drone-units op, de zogenaamde *droneros* (Krame & and Davies, 2023). Islamitische Staat kondigde in 2016 met trots een eigen drone-unit aan die onderzoek naar het gebruik van drones en experimenten met drones op het slagveld moesten organiseren (Doctor, 2025).

Daarnaast spelen een aantal normatieve factoren mee: (3) ideologie of denkbeelden beïnvloeden de afweging om een nieuwe technologie wel of niet te omarmen. Een jihadist heeft mogelijk bijvoorbeeld een voorkeur voor een aanvalsmethode waarbij hij zelf als martelaar zal sterven. Een aanslag met een drone ligt voor een aanslagpleger met zo'n voorkeur minder voor de hand. Ook (4) het zelfbeeld van een organisatie speelt een rol: een groep die zichzelf ziet als bevrijdingsleger ziet grijpt sneller naar conventionele (vuur)wapens, terwijl een verzetsgroep logischerwijs eerder voorkeur zal hebben voor asymmetrische aanvalsmethoden, zoals het plegen van bomaanslagen of gerichte aanslagen op kopstukken van de tegenstander. Ten slotte beïnvloedt (5) de geanticipeerde reactie van de achterban en het bredere publiek ook de adoptiebereidheid: groepen vernieuwen minder snel als zij verwachten dat het gebruik van een nieuwe technologie de legitimiteit bij de eigen achterban of bevolking ondermijnt, of bijvoorbeeld disproportionele reacties van de overheid uitlokt (Lubrano, 2023). Als dreigingsactoren het idee hebben dat het inzetten van een drone voor een aanslag een buitenproportionele hoeveelheid opsporingsaandacht op hen vestigt, of het door hun achterban als een laf middel wordt gezien, zal een actor minder geneigd zijn een drone in te zetten.

Exogene factoren

Exogene factoren liggen in de omgeving rondom de actor. Een belangrijke exogene factor die remmend kan werken op het gebruik van een nieuwe technologie zijn (1) tegenmaatregelen van de overheid. Innovatie door dreigingsactoren is vaak een reactie op beleid: als een overheid doelwitten beter beveiligt, kan een groep nieuwe middelen inzetten om toch effect te sorteren, bijvoorbeeld met behulp van drones.

Tegelijkertijd bepaalt de juridische en praktische werkelijkheid rondom een actor mede het succes van de inzet van zo'n nieuwe technologie. Strenge regulering van drones en onderdelen maakt de succesvolle toepassing ervan door een dreigingsactor moeilijker. In Gaza heeft Hamas bijvoorbeeld moeite met de inzet van drones tegen het Israëlische leger als gevolg van de blokkade van Gaza, waardoor de aanvoer van drones en onderdelen zeer beperkt is (Bouhlaoui, 2025). Voor de kartels in Mexico geldt juist het tegenovergestelde. Zij kunnen relatief makkelijk experimenteren met drones en onderdelen importeren, onder meer omdat in delen van Mexico de staat vrijwel geheel is teruggetrokken, of omdat autoriteiten omkoopbaar zijn, en de kartels zodoende min of meer vrij spel hebben (Ramirez, 2022).

Een tweede exogene factor die een rol speelt zijn (2) (geo)politieke ontwikkelingen. De proliferatie van commerciële drones en hun zichtbare succes in bijvoorbeeld de oorlog in Oekraïne zet druk op actoren om de technologie toe te passen: drones worden makkelijker beschikbaar en hun veronderstelde waarde voor het plegen van aanslagen wordt steeds beter zichtbaar (Bouhlaoui, 2025; Dulligan et al., 2025; Krame & and Davies, 2023).

Gemengde factoren

Naast endogene en exogene factoren die de inzet van drones beïnvloeden bestaan er factoren die de actor met de omgeving verbinden, zogenaamde *gemengde factoren*. Roger (1983) benadrukt, net als Lubrano (2023), de rol van relaties binnen het systeem rond de actor. Allereerst is (1) de relatie met andere (dreigings)actoren van belang. Samenwerking kan innovatie versnellen door uitwisseling van ideeën, tactieken en expertise: via het delen van kennis, het daadwerkelijk trainen van elkaar in het gebruik van een technologie, of de detachering van specialisten van andere kwaadwillende actoren. Rivaliteit tussen actoren kan innovatie ook aanjagen, bijvoorbeeld wanneer een actor met een nieuwe technologie extra aandacht op zich wil vestigen of angst wil creëren, en daarmee een (verondersteld) voordeel behaalt ten opzichte van concurrenten. Ten tweede speelt (2) de relatie tot andere kennisbronnen mee. Kwaadwillende actoren kunnen experts met specifieke vaardigheden of kennis over een innovatie uit de burgerbevolking rekruteren, of leren over een innovatie door andere (open) bronnen te raadplegen.

De aantrekkingskracht van drones

In de voorgaande sectie is besproken welke actorgerelateerde factoren een mogelijke invloed uitoefenen op de beslissing om een innovatie te adopteren. Echter, ook de innovatie zelf speelt een rol: bepaalde technologieën worden sneller geadopteerd omdat zij aantrekkelijker, laagdrempeliger of zichtbaarder zijn dan alternatieven. De volgende sectie richt zich specifiek op karakteristieken van drones als innovatie. Aan de hand van Rogers' (1983) theorie van innovatie worden kenmerken van drones besproken, welke de adoptie ervan door een dreigingsactor waarschijnlijker maken, en onder welke omstandigheden adoptie juist minder waarschijnlijk is. Rogers (1983) onderscheidt vijf kenmerken van innovaties die meespelen bij de keuze om een technologie wel of niet te adopteren. Die karakteristieken zijn: (1) relatief voor- en nadeel, (2) compatibiliteit, (3) complexiteit, (4) beproefbaarheid en (5) observeerbaarheid.

Relatief voor- en nadeel

Met relatief voordeel bedoelt Rogers (1983) dat een potentiële gebruiker van een innovatie het gevoel moet hebben dat inzet van de nieuwe technologie of modus operandi meer oplevert dan bestaande alternatieven. Dat voordeel kan economisch zijn, maar ook liggen in de reputatie die het gebruik van het middel met zich meebrengt, het gebruiksgemak van de technologie, of tevredenheid over de werking ervan. Daarbij gaat het niet alleen om een (objectief) meetbaar voordeel, maar ook om de perceptie van de gebruiker.

Concreet betekent dit voor dreigingsactoren dat de inzet van drones tijdens een voorbereidingshandeling of aanslag wordt afgewogen tegen andere modus operandi: zijn drones relatief goedkoper, trekken ze meer of juist minder aandacht, versterken ze de reputatie van de groep, en worden ze als effectief ervaren? Des te groter het veronderstelde relatieve voordeel van de technologie is, des te sneller dat de technologie zal worden geadopteerd door gebruikers.

De literatuur wijst op uiteenlopende factoren die bepalen in hoeverre drones een relatief voordeel opleveren voor dreigingsactoren. (Commerciële) drones en onderdelen zijn goedkoop en makkelijk verkrijgbaar. Daarnaast zijn er veel varianten: uiteenlopende formaten, payloadcapaciteiten, *first-person-view* (FPV) systemen, met camera's voor voorverkenning, en verschillende reikwijdtes (Bouhlaoui, 2025; Doctor, 2025; Dulligan et al., 2025). Hetzelfde geldt waarschijnlijk voor de beschikbaarheid van vaardige bestuurders; met de hoeveelheid hobbyisten die drones vliegen moet een goede drone-operator in theorie niet lastig zijn om te rekruteren. Dat kan bijvoorbeeld een burger, een specialist uit een oorlogsgebied, of een specialist van een andere, ervaren actor zijn.

Drones kunnen ook tactische voordelen bieden. Ze maken het mogelijk om op afstand te opereren, waardoor de uitvoerder minder fysiek risico loopt dan bij een aanslag of verkenning van dichtbij. De pakkans kan zodoende lager zijn en attributie is mogelijk lastig: zelfs als een drone wordt onderschept, is het niet altijd eenvoudig om de bestuurder te identificeren (Doctor, 2025; Krame & and Davies, 2023). De 'pesterijen' rond Europese militaire bases eind 2025 door (vermoedelijk) statelijke actoren illustreren dit probleem van identificatie en attributie in de praktijk.

Ook kunnen drones functioneren als zogenaamde *force multiplier*, bijvoorbeeld door real-time intelligence te verzamelen en zo een aanslag te coördineren. Terroristische groeperingen doen dit tot nu toe nauwelijks (Bunker et al., 2020; Doctor, 2025), maar de kartels in Mexico integreren drones volgens sommige onderzoekers wel in dit soort *combined arms*-operaties: van verkenning en coördinatie ter voorbereiding van een aanval, tot drones die de vijand met explosieven bestoken terwijl grondtroepen operaties uitvoeren (Bunker & Sullivan, 2021b; Parcover, 2025). Tegelijkertijd vergen dit soort operaties aanzienlijke vaardigheden, mankracht en coördinatie. Dit soort toepassingen zijn om die reden minder aantrekkelijk voor groepen met weinig mensen en middelen, en simpelweg onhaalbaar voor eenlingen (Doctor, 2025).

Drones bieden mogelijk ook een strategisch voordeel voor bepaalde actoren; namelijk de psychologische impact van (aanslagen met) drones. Controle over het luchtruim geldt doorgaans als symbool voor de macht van de overheid. Drones kunnen die hegemonie van de overheid over het luchtruim in twijfel trekken (Bouhlaoui, 2025; Doctor, 2025; Dulligan et al., 2025; Veilleux-Lepage & Archambault, 2022). Daarnaast creëert de onvoorspelbaarheid van drones en hun geluid ook aanzienlijke psychologische impact. Het gezoem en het rondhangen van drones kan het gevoel creëren dat er op elk moment, onverwachts, een aanval uit de lucht kan komen. Het filmen en verspreiden van beelden van droneaanslagen door bijvoorbeeld Hamas tijdens de aanslagen van 7 oktober, of door de kartels in Mexico, draagt op deze manier bij aan een vorm van psychologische oorlogsvoering (Bouhlaoui, 2025; Bunker & Sullivan, 2021b; Veilleux-Lepage & Archambault, 2022).

Een aanslag met een drone vereist naast een drone ook een werkend explosief. Het verkrijgen of vervaardigen van een explosief vergroot het risico dat een kwaadwillende actor wordt opgepakt.

Een ander strategisch voordeel voor kwaadwillende actoren komt voort uit het feit dat overheden momenteel beperkt grip op drones lijken te hebben. Wet- en regelgeving, inkoopbeperkingen, en de uitrol van counterdronecapaciteit lopen vaak achter op de praktijk. Traditionele luchtverdedigingssystemen werken bovendien slecht tegen drones, omdat drones lage radar- en warmtesignalen afgeven en op lage hoogtes vliegen (Bouhlaoui, 2025; Krame & and Davies, 2023). Counterdronesystemen vereisen daardoor een vrij specifieke combinatie van onder meer speciale radar-, RF- en infraroodsystemen, optische en akoestische sensoren voor detectie, en middelen zoals jammers, netten en lasers om drones te neutraliseren. Deze systemen zijn complex en kostbaar om uit te rollen en te bemannen (Doctor, 2025; Dulligan et al., 2025), zeker wanneer er veel mogelijke doelwitten tegelijk beveiligd moeten worden. Hierdoor ontstaat een asymmetrisch voordeel voor dreigingsactoren: drones zijn relatief goedkoop, terwijl mitigerende maatregelen grote investeringen van politie en defensie vragen (Doctor, 2025; Krame & and Davies, 2023).

Tegenover deze voordelen van de inzet van drones staan ook enkele nadelen. Allereerst kan het inzetten van een drone de pakkans vergroten, zeker rond zwaarbeveiligde objecten met dronedetectie. Veel commerciële drones hebben een beperkte reikwijdte en vereisen zodoende dat de operator relatief dicht bij het doelwit blijft. Hoe langer een operatie met zo'n drone duurt, des te groter de kans dat de drone of operator worden opgemerkt en uitgeschakeld door de autoriteiten (Doctor, 2025). In zulke contexten is het mogelijk eenvoudiger voor een dreigingsactor om bijvoorbeeld een explosief te plaatsen, of een voertuig of vuurwapen te gebruiken.

Een tweede nadeel is dat alternatieve middelen voor veel actoren eenvoudiger beschikbaar zijn. Voor criminelen kost het vermoedelijk minder moeite om een vuurwapen te regelen of een uitvoerder van een liquidatie in te huren, dan een geschikte drone te kopen, aan te passen, en een operator te vinden, te trainen, en de operatie uit te laten voeren. Bovendien is voor een aanslag niet alleen een drone nodig, maar ook een payload. In Nederland, waar explosieven en precursoren voor zelfgemaakte explosieven zwaar gereguleerd zijn, kan het proberen aan te schaffen van deze middelen de pakkans verder verhogen (Doctor, 2025). Ook maken wet- en regelgeving en de verdere uitrol van counterdronesystemen sommige doelwitten moeilijker bereikbaar dan met meer conventionele middelen.

Compatibiliteit

Naast het relatieve voor- of nadeel van een innovatie, wijst Rogers (1983) op de *compatibiliteit* van de nieuwe technologie met bestaande waarden, bestaande kennis en ervaring, en de behoeften van potentiële gebruikers. Een technologie wordt sneller omarmd door een dreigingsactor als deze aansluit bij de waarden en behoeften van de actor of organisatie.

Een belangrijk compatibiliteitsvoordeel van drones is veelzijdigheid. Drones zijn inzetbaar in meerdere fasen van de aanvalscyclus: in de voorverkenning of ter ondersteuning van een aanslag, of voor een aanslag zelf. Daarmee sluiten drones aan bij uiteenlopende werkwijzen en behoeften. Ook de variëteit in drones, van commerciële drones tot militaire drones, en *fixed-wing* tot *rotary-wing* modellen, versterken deze veelzijdigheid.

Daarnaast is het voorstelbaar dat actoren die het strategische doel hebben om de legitimiteit van de staat te ondermijnen, of ernstige angst onder de bevolking willen zaaien, relatief snel naar drones grijpen. In Nederland zou een drone-aanslag waarschijnlijk veel media-aandacht genereren. Voor terroristen of eenlingen die uit zijn op veel maatschappelijke impact, kan die veronderstelde aandacht een reden zijn om drones te gebruiken bij een aanslag. Bouhlaoui (2025) trekt een vergelijking met de populariteit van voertuigen als aanslagmiddel voor eenlingen, en stelt dat de combinatie van de wijdverspreide beschikbaarheid van drones en de veronderstelde symbolische impact van een incident, het plegen van een aanslag met een drone extra aantrekkelijk voor hen kan maken. Voor een rechtsextremistische terreurgroep zoals The Base, die via het *leaderless resistance*-model proberen zo lang mogelijk uit handen van de autoriteiten te blijven en strategische doel hebben disruptie te veroorzaken met aanslagen op overheidsfunctionarissen en kritieke infrastructuur (Rai, 2025), sluiten de operationele voordelen van drones goed aan op de doelen en voorkeursmiddelen van de organisatie.

Ook op het gebied van compatibiliteit zijn er nadelen. Het gebruiken van een drone kan botsen met de doelen van actoren die geven om hun levensvatbaarheid en daarom onnodige aandacht willen vermijden. Waar terroristen publiciteit mogelijk juist nastreven, kunnen statelijke actoren of criminele organisaties een drone-aanslag juist vermijden, omdat die waarschijnlijk meer politieke en opsporingsaandacht oproept dan conventionele aanslagmethoden waar autoriteiten en burgers al meer aan "gewend" zijn.

Ook sluit het gebruik van een drone bij een aanslag, zoals Lubrano's (2023) model van innovatie ook veronderstelt, niet altijd aan bij de waarden of het zelfbeeld van een actor. Jihadisten streven regelmatig het martelaarschap na, bijvoorbeeld door zelfmoordaanslagen met explosieven te plegen (Moghadam, 2008). Daarnaast zijn eenlingen die geweld plegen regelmatig suïcidaal of gedreven door een drang naar erkenning, waardoor zij juist zelf in de vuurlinie willen staan en bijvoorbeeld tijdens het plegen van een massaschietpartij willen sterven (Silva & Lankford, 2024). Ten slotte kan het voor criminele organisaties van belang zijn om iemand – in het openbaar en voor de ogen van omstanders – te liquideren, om zo een boodschap af te geven (van Gestel & Kouwenberg, 2021). In zulke gevallen sluit een drone niet aan bij de strategische doelen of het zelfbeeld van de actor, en is het dus geen logische voorkeursmethode voor een aanslag.

Complexiteit

Complexiteit is volgens Rogers (1983) de mate van veronderstelde gebruiksvriendelijkheid van een innovatie. Hoe eenvoudiger de technologie, hoe groter de kans op adoptie. Bij drones verlaagt gebruiksvriendelijkheid – makkelijke besturing en intuïtieve interfaces, programmeerbaarheid, en de al dan niet eenvoudige montage van een payload – de drempel voor dreigingsactoren om de technologie in te zetten. Op het gebied van complexiteit is een voordeel dat er veel soorten drones zijn: van *quadcopters* tot *fixed-wing* modellen, en van kleine hobbydrones tot industriële drones die veel gewicht kunnen dragen. Drones zijn bovendien te modificeren. Met 3D-printers kunnen aflevermechanismen of projectielen relatief eenvoudig worden aangepast om payloads effectiever bij een doelwit te krijgen.

Daar staat tegenover dat het tijd en moeite kost om drones effectief te integreren in de aanvalscyclus. De inzet door Islamitische Staat en Mexicaanse kartels verliep gefaseerd: eerst werden ze ingezet voor smokkel en verkenning, daarna werd er geoefend met payloads, en pas uiteindelijk vond er schaalvergroting voor de daadwerkelijke inzet van drones voor aanslagen plaats. Dit proces duurde jaren en laat zien dat inzet voor aanslagen complex is en veel lerend vermogen vereist (Bouhlaoui, 2025; Bunker & Sullivan, 2021b). Haugstvedt (2021) suggereert daarom dat grotere georganiseerde actoren logischerwijs vroege gebruikers van drones waren – mede door hun grote capaciteit en de beperkte repressie door de autoriteiten in de gebieden waarin ze opereerden.

Drones zijn relatief complex: het is voor veel actoren simpelweg makkelijker of aantrekkelijker om een mes, vuurwapen of voertuig te gebruiken voor een aanslag.

Voor actoren met beperkte capaciteit zijn drones mogelijk ook vooral bruikbaar in de verkenningsfase. Het uitvoeren van een aanslag vereist namelijk meer dan alleen het kunnen besturen van een drone. Een actor moet ook in staat zijn om explosieven te verkrijgen of zelf te vervaardigen uit precursoren, en om deze vervolgens effectief bij het doelwit te krijgen. Dit vereist technische vaardigheden en werkende aflever- en ontstekingsmechanismen (Doctor, 2025). Bij quadcopters gaat het daarbij vaak om (zelfgemaakte) aflevermechanismen en aangepaste projectielen, al dan niet via 3D-printing vervaardigd, waarmee een payload gecontroleerd en met enige precisie kan worden afgeworpen (Haugstvedt, 2021). De benodigde kennis en vaardigheden op het gebied van explosieven en aflevermechanismen vormen daardoor voor sommige actoren een belemmering om drones daadwerkelijk voor een aanslag in te zetten.

Tegelijkertijd zijn de technologische ontwikkelingen rondom drones sinds 2021 snel gegaan, waardoor de *barrier-to-entry* inmiddels ook lager is voor actoren met beperkte capaciteit. De proliferatie van drones op slagvelden zoals Oekraïne en de bijkomende technologische ontwikkelingen maakt het waarschijnlijk dat drones in de toekomst nog gebruiksvriendelijker en nog makkelijker aan te passen worden – ook voor aanslagen (Bouhlaoui, 2025). Technologieën zoals AI en machine learning, target-lock systemen en swarm-technologie zullen de complexiteit van de inzet van drones voor aanslagen waarschijnlijk verlagen (Bouhlaoui, 2025; Dulligan et al., 2025).

Tot slot moet op het gebied van complexiteit echter ook het alternatieven-argument benadrukt worden. Drones kunnen niet alleen complex zijn; het is voor veel actoren simpelweg makkelijker om een mes, vuurwapen of voertuig te vervaardigen en te gebruiken (Nationaal Coördinator Terrorismebestrijding- en Veiligheid, 2024). De operationele kennis van het gebruik van alternatieve middelen en de ervaring met alternatieve modus operandi zijn voor veel actoren beter ingebed in het (organisatorisch) geheugen. De aantrekkingskracht van alternatieve, simpelere aanvalsmethoden zal dus een remmende werking op de inzet van drones bij een aanslag hebben.

Beproefbaarheid

Beproefbaarheid gaat over de mogelijkheid om met een technologie te experimenteren voordat deze volledig wordt omarmd. Technologieën waar op laagdrempelige wijze mee geëxperimenteerd en geoefend kan worden, worden sneller geadopteerd (Rogers, 1983).

De omgevingscondities op het gebied van de beproefbaarheid van drones zijn enerzijds gunstig en anderzijds ongunstig. In Nederland gebruiken hobbyisten drones op grote schaal. Ondanks wet- en regelgeving en registratievereisten zullen de autoriteiten niet snel opkijken van iemand die op normale locaties oefent met het besturen van een drone. Daarnaast is bekend dat dreigingsactoren ook in Nederland drones testen tijdens het plegen van minder risicovolle delicten, zoals drugssmokkel bij gevangenissen (Dienst Justitiële Inrichtingen, 2022). Dit soort toepassingen bieden dreigingsactoren echte scenario's waarin operators (onder enige druk om gepakt te worden) kunnen oefenen met het afleveren van een payload – in dit geval smokkelwaar – en leren hoe ze een beveiligd doelwit kunnen bereiken en onvindbaar kunnen blijven. Via *learning-by-doing* bouwen zij zo kennis op die later ook voor andere doeleinden inzetbaar is. Gezien de evolutie bij Mexicaanse kartels – van smokkel naar aanslagen en gecoördineerde aanvallen (Bunker & Sullivan, 2021b) – is zo'n ontwikkeling voorstelbaar.

Tegelijkertijd brengt het experimenteren met drones ook nadelen met zich mee. Door de huidige alertheid rond drones binnen het Nederlandse veiligheidsdomein kan oefenen – zeker in de buurt van beveiligde objecten – mogelijk snel tot detectie en opvolging leiden. Die bewustwording kan actoren afschrikken en ertoe leiden dat zij eerder kiezen voor bestaande middelen voor verkenning en intelligence, zoals uit open bronnen of door middel van (menselijke) observatie.

Observeerbaarheid

Ten slotte betreft *observeerbaarheid* volgens Rogers (1983) de zichtbaarheid van succesvolle toepassingen van een technologie. Hoe meer potentiële gebruikers zien dat de inzet van een innovatie resultaten oplevert, hoe waarschijnlijker het wordt dat zij die technologie zelf gaan gebruiken.

De oorlog in Oekraïne heeft het succesvolle gebruik van drones zeer zichtbaar gemaakt en daarmee waarschijnlijk de perceptie van effectiviteit en gebruiksgemak ervan bij dreigingsactoren veranderd (Bouhlaoui, 2025). Ook zichtbare toepassingen door andere dreigingsactoren buiten conflictgebieden, zoals door de kartels in Mexico, tonen de mogelijke voordelen van dronegebruik voor andere dreigingsactoren (Doctor, 2025; Krame & and Davies, 2023). Dit effect wordt versterkt door de productie en verspreiding van propaganda. Zowel Islamitische Staat als Mexicaanse kartels hebben dronegebruik expliciet uitgelicht in propaganda om slagkracht te tonen (Bunker & Sullivan, 2021a; Veilleux-Lepage & Archambault, 2022). De succesvolle inzet van drones voor het plegen van een aanslag in het Westen, vooral als deze gepaard gaat met veel publiciteit, zal de observeerbaarheid waarschijnlijk nog meer doen vergroten. Als actoren zien dat anderen aantoonbaar succes behalen met het gebruiken van drones ten behoeve van een aanslag, kan adoptie versnellen en mogelijk exponentieel toenemen.

Een tegenargument op het gebied van observeerbaarheid betreft de zichtbaarheid van mitigerende maatregelen van de overheid. Naar aanleiding van bijvoorbeeld de drone-pesterijen rond militaire bases in Nederland en andere delen van Europa is in de media breed uitgemeten dat overheden groot inzetten op counterdronemiddelen. Hierdoor kunnen dreigingsactoren besluiten drones niet in te zetten, om opsporingsdruk en repressie te voorkomen.

Resumerend

Een breed scala aan factoren kan vanuit theoretisch perspectief bijdragen aan het verklaren van zowel adoptie als non-adoptie van drones voor het plegen van een aanslag. In de voorgaande sectie zijn de belangrijkste argumenten voor adoptie en non-adoptie besproken, gebaseerd op Rogers' (1983) vijf karakteristieken van innovaties en de bredere literatuur over het gebruik van drones door dreigingsactoren. Deze inzichten zijn samengebracht in een theoretisch kader (tabel 3). Dit kader biedt een gestructureerde manier om inzicht te krijgen in de mogelijke overwegingen die dreigingsactoren maken bij de keuze om wel of geen drone in te zetten voor het plegen van een aanslag. Het afwegingskader maakt daarmee niet zozeer individuele beslissingen voorspelbaar, maar helpt om relevante factoren systematisch te ordenen en vergelijkbaar te maken tussen actoren en casussen.

Daarbij zijn twee belangrijke nuanceringen van toepassing. Ten eerste wordt niet gepretendeerd dat dit afwegingskader een volledig of sluitend overzicht is. Het betreft een verkennend analytisch instrument, dat op basis van aanvullende empirische bevindingen, expertinzichten en verdere literatuur kan worden aangescherpt of uitgebreid.

Ten tweede gaat het afwegingskader impliciet uit van een zekere mate van rationaliteit in besluitvorming, terwijl in de praktijk keuzes ook (deels) onbewust of intuïtief tot stand kunnen komen. Dit betekent ook dat de in het kader genoemde voor- en nadelen per karakteristiek niet wederzijds exclusief zijn en dat hun onderlinge 'weging' door de lezer niet als absoluut moet worden geïnterpreteerd. Een actor kan voor- en nadelen als even zwaar ervaren en desondanks tot een specifieke keuze komen.

Ten slotte dient expliciet te worden benadrukt dat dit een overkoepelend kader betreft. De relatieve zwaarte van de verschillende factoren zal naar verwachting variëren per type dader, mede afhankelijk van actor-gerelateerde kenmerken zoals beschreven door Lubrano (2023). Zo maken terroristische organisaties fundamenteel andere afwegingen dan eenlingen, evenals ten opzichte van criminele organisaties en statelijke actoren. Dit afwegingskader is bovendien waarschijnlijk vooral toepasbaar op niet-statelijke actoren, aangezien het is gebaseerd op literatuur over het gebruik van drones door dergelijke actoren.

Tabel 3: Theoretisch afwegingskader voor dreigingsactoren om drones wel of niet te implementeren
Naar Rogers' (1983) model van diffusie van technologie en bredere literatuur over drones

Karakteristiek	Korte uitleg	Voordeel (mogelijke aantrekkelijkheid van drones)	Nadeel (mogelijke barrières voor gebruik van drones)
Relatief voor- en nadeel	Mate waarin drones als beter middel voor een aanslag worden gezien dan alternatieve middelen en methoden	• Relatief goedkoop en breed inzetbaar • Veel variatie in type en inzet (grootte, snelheid, doelen) • Veel vaardige bestuurders beschikbaar • Inzet op afstand verlaagt risico voor gebruiker • (Mogelijk) moeilijker te detecteren • Asymmetrisch voordeel tegen *hard targets* • Kan luchtoverwicht van overheid uitdagen • Sterke psychologische impact op burgers en autoriteiten • Beperkte wetgeving en counter-UAS-capaciteit creëren ruimte voor inzet	• Naast drone is (voor aanslag) ook payload/ explosief nodig • Alternatieven kunnen praktischer zijn • Detectie, jamming en counter-UAS kunnen effectiviteit beperken • Wet- en regelgeving kan aanschaf en inzet bemoeilijken • Amateuristische inzet kan kans op detectie vergroten • Succesvolle inzet kan extra aandacht en repressie uitlokken
Compatibiliteit	Mate waarin drones passen bij bestaande modus operandi, waarden en strategische voorkeuren van een actor	• Goed in te passen in bestaande aanvalscycli • Multi-inzetbaar: voorverkenning, (logistieke) ondersteuning, aanslagmiddel • Aan te passen aan specifieke behoeften	• (Effectieve) integratie in aanvalscyclus kost tijd, capaciteit en lerend vermogen • Inzet kan botsen met ideologie, waarden of voorkeuren
Complexiteit	Hoe moeilijk het is om drones effectief te beheersen, te gebruiken voor het beoogde doel, en in te passen in bestaande aanvalscycli en modus operandi	• Relatief gebruiksvriendelijk, ook voor niet-specialisten • Ontwikkelingen verlagen drempels; besturing wordt makkelijker en intuïtiever • AI/target lock/zwermtechnologie kan complexiteit verder verminderen	• Effectieve inzet vereist training en operationele kennis • Alternatieve aanslagmethoden zijn vaak eenvoudiger • Voor aanslag is extra kennis en kunde nodig (van aflevermechanismen, ontstekingsmechanismen en explosieven) • Aanpassen van een drone kan met beperkte kennis en vaardigheden moeilijk zijn
Beproefbaarheid	Mate waarin met drones geëxperimenteerd en geoefend kunnen worden voordat inzet bij een daadwerkelijke aanslag volgt	• Oefenen is laagdrempelig door beperkte restricties • Testen van dry-runs in echte scenario's kan ook met alternatieve payloads (smokkel in gevangenissen)	• Experimenteren, trainen of dry-runs kunnen leiden tot vroegtijdige detectie
Observeerbaarheid	Zichtbaarheid van succes van toepassingen van drones voor aanslagen in andere contexten	• Succesvolle inzet in conflicten stimuleert imitatie • Propaganda verlaagt drempels en werkt legitimerend • Online handleidingen en instructies verlagen drempel voor gebruik • Kennis verspreidt zich mogelijk via training, rekrutering en uitwisseling • Rekrutering van experts (bijv. veteranen) versnelt toepassing	• (Indirect) grotere zichtbaarheid kan ook leiden tot meer tegenmaatregelen door de overheid

Leer- en innovatieroutes voor dreigingsactoren

In de voorgaande sectie zijn de factoren op actor- en technologieniveau besproken die van invloed kunnen zijn op de adoptie van drones door dreigingsactoren. Een laatste element van het theoretisch kader betreft de wijze waarop dreigingsactoren met een nieuwe technologie in aanraking komen. In deze sectie wordt daarom ten slotte stilgestaan bij de vraag hoe dreigingsactoren kennisnemen van en leren omgaan met technologieën zoals drones. Daarbij wordt verder voortgebouwd op Rogers' (1983) innovatietheorie en de bestaande literatuur over dronegebruik door dreigingsactoren, met aandacht voor verschillende leer- en innovatieroutes.

Allereerst kan een actor zelf met drones *experimenteren*. Dit betekent dat een actor een drone aanschaft of zelf produceert, en zelf gaat oefenen met vliegen en bijvoorbeeld het aanpassen van de drone om een payload te bevestigen. Vooral vroege gebruikers van een technologie worden gedwongen om te experimenteren, omdat ze nog niet kunnen leren van (succesvolle voorbeelden van) anderen (Rogers, 1983). Bij dronegebruik door dreigingsactoren staan vooral het CJNG-kartel, Hamas, Hezbollah en Islamitische Staat bekend als vroege gebruikers. Hamas en Hezbollah probeerden relatief vaak zelf drones te ontwikkelen, terwijl het CJNG-kartel en Islamitische Staat vooral experimenteerden met het modificeren van commerciële drones voor aanslagen (Bouhlaoui, 2025; Bunker et al., 2020; Veilleux-Lepage & Archambault, 2022).

Ten tweede kunnen actoren leren door te *observeren* en zo (indirect) van elkaar te leren. Sociale media staan vol met informatie over het gebruik van drones in het conflict in Oekraïne: talloze kanalen delen beelden van succesvolle inzet van drones, technische uitleg over aanpassingen aan drones, en tactische analyses. Datzelfde geldt voor het gebruik van drones door Islamitische Staat en de Mexicaanse kartels. Potentiële gebruikers krijgen daarmee in feite een soort blauwdruk om toepassingen van drones die in andere contexten succesvol blijken te kopiëren (Bouhlaoui, 2025). Doctor (2025) beargumenteert dat de gefaseerde diffusie van dronegebruik door dreigingsactoren door zo'n proces van kennisdeling via open bronnen wordt gekenmerkt. De zogenaamde *innovatoren*, zoals bijvoorbeeld ISIS, adopteren een technologie vroeg en experimenteren ermee, waarna een grotere groep *vroege gebruikers* volgt zodra de werking in de praktijk zichtbaar is – bijvoorbeeld de kartels in Mexico. Naarmate het gebruik van drones normaliseert en de kennis over de toepassing van drones breder beschikbaar wordt, sluit ook de *vroege meerderheid* aan; de Taliban, Houthi's, HTS, de FARC en de rebellen in Myanmar. Hierna volgen ook de *late meerderheid* en *laatkomers*. Hierdoor groeit het aantal gebruikers niet geleidelijk, maar exponentieel (Moore & McKenna, 2001; Rogers, 1983). In lijn met de verwachtingen van Doctor (2025) en Rogers (1983) zullen er op termijn dus exponentieel meer dreigingsactoren gebruik gaan maken van drones ten behoeve van een aanslag.

Een actor kan ook direct leren van andere dreigingsactoren door middel van *training*. Het is niet ondenkbaar dat zulke kruisbestuiving tussen actoren plaatsvindt. Doctor (2025) en Veilleux-Lepage en Archambault (2022) noemen beiden dat er al een directe uitwisseling van kennis over drones bestaat tussen Iran-gelieerde terroristische groeperingen, zoals de Houthi's, Hezbollah en Palestijnse Islamitische Jihad. Ook bestaan er al langer vermoedens dat bijvoorbeeld de Mexicaanse kartels hun mensen laten trainen door Hezbollah of de Colombiaanse FARC, voor onder andere het bouwen van tunnels en het ontwikkelen van explosieven (Krame & and Davies, 2023). Het is voorstelbaar dat de directe uitwisseling van expertise ook bij drones kan plaatsvinden. Leunen op andermans' kennis beperkt voor dreigingsactoren risico's en verkort de tijd tussen het idee en de uitvoering van een aanslagpoging. In plaats van zelf langdurig kennis op te bouwen via *trial-and-error*, kunnen actoren terugvallen op bestaande expertise van anderen (Doctor, 2025; Rogers, 1983).

Dreigingsactoren nemen kennis van en leren omgaan met drones door te experimenteren, te observeren, elkaar te trainen, of door experts te rekruteren.

Ten slotte kan een actor experts inhuren of *rekruteren*. Dit kan gaan om gedetacheerde leden van andere dreigingsactoren. Daarnaast kunnen burgers met specialistische kennis worden gerekruteerd. In Nederland is het bekend dat er uitwisseling van kennis en expertise is tussen de Nederlandse georganiseerde misdaad en Mexicaanse kartels, bij bijvoorbeeld de productie van crystal meth en het in- en uitwassen van cocaïne (Davidse, 2024). In het licht van drones kan ook worden gedacht aan de rekrutering van personen met een achtergrond in bouwkunde en techniek, of defensie en politie. Eén van de eerste arrestaties van ingehuurde drone-experts in Mexico (door het Cartel de Santa Rosa) betrof twee bouwkundestudenten (Krame & and Davies, 2023). Voor (rechts)extremistische groeperingen vormen ex-leden van defensie en politie al een voedingsbodem om operationele en technische kennis binnen te halen (Haugstvedt, 2021; Van Dongen et al., 2022), hetgeen in het licht van drones zorgwekkend kan zijn. Immers, in veel landen zet defensie en politie nu vol in op drones, waardoor er een grote vijver van potentiële rekruten ontstaat. Een recent incident lijkt te illustreren dat zulke experts inderdaad een rol kunnen spelen bij droneaanslagen. In Rusland werd onlangs een moordaanslag gepleegd met een FPV-drone op een vermogend zakenman. Dit incident is opmerkelijk, omdat het het allereerste voorbeeld is van een succesvolle aanslag met een drone op een persoon buiten het conflictgebied in Oekraïne. De autoriteiten vermoeden dat de dader een veteraan uit de oorlog in Oekraïne is (Jager, 2025).

Tabel 4: Mogelijke leer- en innovatieroutes voor dronegebruik door dreigingsactoren

Experimenteren	Observeren	Training	Rekruteren
Actoren verwerven of bouwen drones en ontwikkelen kennis over het gebruik of de doortontwikkeling van drones door zelf te experimenteren en te oefenen. Deze innovatieroute is vooral kenmerkend voor vroege gebruikers.	Actoren leren via open bronnen zoals sociale media, beelden en analyses van dronegebruik in van conflictgebieden, of het gebruik van drones door andere dreigingsactoren. Op deze wijze kunnen succesvolle toepassingen van drones ten behoeve van een aanslag snel worden gekopieerd en opgeschaald.	Kennis en ervaring worden doelgericht uitgewisseld tussen dreigingsactoren, bijvoorbeeld via het direct delen van instructies en expertise, of het detacheren van experts. Hierdoor nemen de risico's bij het gebruik van drones af, omdat eigen experimentatie voor een succesvolle toepassing niet langer nodig is.	Actoren trekken externe specialisten aan door hen te rekruteren of in te huren (bijv. technici, ingenieurs, hobbypiloten of veteranen). Zo vullen zij snel ontbrekende operationele en technische kennis aan, beperken zij risico's en verkorten zij de leercyclus die gepaard gaat met het zelf experimenteren met drones.

Deel II: Empirische studie

Naast een theoretische bijdrage over factoren die dronegebruik door dreigingsactoren mogelijk bevorderen en belemmeren, beoogt deze studie ook een empirische bijdrage te leveren. In openbare stukken wordt vaak gesuggereerd dat incidenten met drones nauwelijks voorkomen (Nationaal Coördinator Terrorismebestrijding- en Veiligheid, 2024; van Oosten, 2025). Echter, bestaande studies naar dronegebruik door dreigingsactoren zijn vaak exploratief of gebaseerd op literatuuronderzoek (Bouhlaoui, 2025; Damiani & Jasper, 2024; Doctor, 2025). Empirische studies zijn schaars en kennen hun beperkingen: zo richt de studie van Veilleux-Lepage en Archambault (2022) zich voornamelijk op incidenten buiten het Westen, terwijl het incidentenoverzicht van Haugstvedt (2024) zich enkel op geslaagde aanslagen richt waarbij drones als explosief werden ingezet, en omvat deze dataset geen pogingen tot aanslagen of toepassingen die een aanslag ondersteunen, zoals bijvoorbeeld het verkennen van een doelwit ten behoeve van het plegen van een aanslag. Daarnaast ontbreken in deze dataset enkele incidenten die in de huidige studie zijn geïdentificeerd. De huidige studie vult deze literatuur aan door een empirisch overzicht te bieden dat zich specifiek richt op het Westen en zowel aanslagen op personen of objecten als plannen daarvoor omvat, evenals toepassingen van drones ter ondersteuning of voorbereiding van een aanslag.

Methode

Vanwege het beperkte empirische onderzoek naar dronegebruik door dreigingsactoren in het Westen, en de veronderstelling dat het gebruik van drones in andere contexten door specifieke omgevingsfactoren vaker voorkomt (bijvoorbeeld omdat explosieven makkelijker beschikbaar zijn omdat de drone in een oorlogssituatie wordt toegepast), volgt deze vergelijkende studie een verkennende en inductieve benadering. In plaats van het toetsen van hypothesen uit de bestaande literatuur beoogt het onderzoek patronen te identificeren in nieuwe, systematisch verzamelde data over het gebruik van drones door dreigingsactoren in het Westen.

De ontwikkeling van het codeboek waarmee de data is geanalyseerd vond iteratief en abductief plaats: codes zijn deels ontwikkeld op basis van de geraadpleegde theorie en literatuur. Een ander deel van de codes is ontwikkeld door het analyseren van bronmateriaal over cases, waarna verdere relevante variabelen werden geïdentificeerd die geschikt waren voor dataverzameling. Vervolgens werd het codeboek toegepast op een volgende casus om te beoordelen of aanvullende variabelen konden worden onderscheiden. Dit proces is herhaald totdat er geen nieuwe variabelen meer naar voren kwamen. Een samengevatte versie van het codeboek is opgenomen in Appendix A.

Cases zijn geïdentificeerd aan de hand van een systematische zoekstrategie. Hierbij zijn zoektermen die gerelateerd zijn aan drones en het gebruik hiervan door dreigingsactoren ingevoerd in Google. Er is gewerkt met een vaste lijst van zoekstrings, waarin termen zoals ‘aanslag’, ‘aanslagplannen’, ‘aanval’ en ‘terrorisme’, evenals variaties hierop, systematisch zijn gecombineerd met drone-gerelateerde zoekwoorden. Deze zoekopdrachten zijn uitgevoerd over de gehele onderzoeksperiode (2010 – 2025). Om de dekking te vergroten, zijn deze zoekopdrachten uitgevoerd in de oorspronkelijke talen van de onderzochte landen, waarbij gebruik is gemaakt van vertalingen via Google Translate en OpenAI’s ChatGPT-5 (5.0, 5.1 & 5.2). De zoekstrategie richtte zich specifiek op toonaangevende nieuwsmedia, waarbij per land de twee meest populaire kranten zijn meegenomen. Daarnaast zijn relevante drone-gerelateerde websites, zoals het platform DroneWatch, geraadpleegd. Waar mogelijk zijn meerdere bronnen per casus geraadpleegd ter verificatie. De dataverzameling is voortgezet totdat verzadiging optrad en geen nieuwe relevante cases werden aangetroffen. In totaal werden 34 incidenten in de periode 2010 tot en met 2025 geïdentificeerd.

Inclusie- en exclusiecriteria

Deze studie richt zich uitsluitend op dronegebruik door dreigingsactoren in het Westen, vanaf 2010 tot en met 2025. Met het Westen wordt in de context van deze studie bedoeld: landen die deel uitmaken van de Europese Unie of de Europese Economische Zone, en landen wereldwijd waar Engels de meest gesproken taal is; de Verenigde Staten, Canada, Australië en Nieuw-Zeeland.

Er is een conservatieve benadering van hetgeen dat “incidenten met drones” omvat gehanteerd. De studie beperkt zich tot incidenten die gericht zijn op het plegen van aanslagen op personen of objecten. Kortom, uit het model van Veilleux-Lepage en Archambault (2022) zijn alleen toepassingen geselecteerd waarbij het gebruik van de drone het doel had om een aanslag te plegen of een aanslagpoging te

ondersteunen; waaronder ISR-toepassingen, logistieke ondersteuning bij een aanslag, het verstoren van activiteiten van beveiligingsmaatregelen tijdens het plegen van een aanslag, of het plegen van een aanslag zelf. Communicatie-gerelateerde toepassingen van drones uit het model van vallen af. Het smokkelen van contrabande in penitiaire inrichtingen is ook niet meegenomen, tenzij het wapens betreft die (mogelijk) voor een aanslag in de gevangenis worden gebruikt. Incidenten waarbij het niet mogelijk is om de intentie (poging tot aanslag of ondersteuning daarbij) van de gebruiker te achterhalen (zoals bijvoorbeeld de vele observaties van drones rondom vliegvelden en militaire bases in Europa), zijn ook niet meegenomen in de dataset.

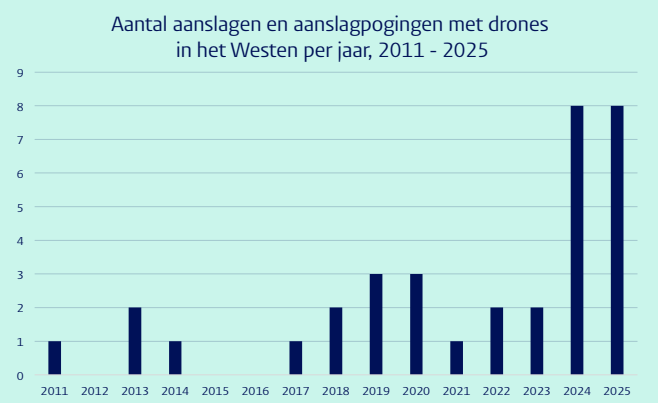
Ook zijn incidenten met drones in de onderzochte landen, die onderdeel zijn van een gewapend conflict buiten de bestudeerde landen, niet opgenomen in de dataset. Om deze reden vielen verschillende incidenten af, zoals verschillende aanslagen met drones op tankers van de Russische schaduwvloot in Griekse wateren. Ook werden drie incidenten tussen 2017 en 2025 geïdentificeerd waarbij cellen van Islamitische Staat, Hamas en Hezbollah, onderdelen van drones in Europa inkochten om die vervolgens naar conflictgebieden in Libanon, Gaza en Syrië te verschepen. Ook enkele incidenten waarbij verdachten in Canada en Duitsland onderdelen van drones verscheepten naar Rusland ter ondersteuning van hun oorlog in Oekraïne, zijn om deze reden niet opgenomen. Er werd één incident geïdentificeerd waar een rechtsextremistische groep tijdens Pride in Zürich anti-LGBTQ+ flyers verspreidde met een drone. Ten slotte werden twee incidenten in Canada (2015, 2022) geïdentificeerd waarbij werd vermoed dat er een wapen een gevangenis in was gesmokkeld met een drone om een aanslag te plegen. Echter, latere berichtgeving bevestigde dat – na een uitgebreide zoektocht – de wapens niet waren gevonden. Deze incidenten zijn ook niet opgenomen in de dataset.

Bronnen

De dataset die de basis vormt voor de analyse van de incidenten, is uitsluitend gebaseerd op open bronnenmateriaal. Het betreft voornamelijk journalistieke bronnen, zoals lokale en landelijke kranten. De nieuwsbronnen die in de fase van casusselectie zijn geïdentificeerd, zijn in een vervolgstap systematisch uitgebreid met aanvullende berichtgeving uit andere (met name lokale) nieuwsmedia. Dit is gedaan door per geïdentificeerde casus verder te zoeken met zoektermen die specifiek gerelateerd waren aan het incident in kwestie. Vervolgens is nagegaan of er officiële verklaringen over het incident beschikbaar waren, bijvoorbeeld van de politie, veiligheidsdiensten of het openbaar ministerie in het desbetreffende land. Waar mogelijk is mediaberichtgeving met dergelijke primaire bronnen aangevuld ter verificatie en verdieping. Er zijn geen pogingen ondernomen om informatie over daders of verdachten te verzamelen via sociale media of andere vormen van open-source dataverzameling buiten reguliere nieuws- en institutionele bronnen. Bronnen die niet in het Engels, Nederlands of Duits beschikbaar waren, zijn vertaald met behulp van Google Translate of OpenAI's ChatGPT-5 (5.0, 5.1 & 5.2). De zoekstrategie leidde tot de identificatie van 194 unieke primaire bronnen die betrekking hadden op de incidenten uit de dataset.

Resultaten

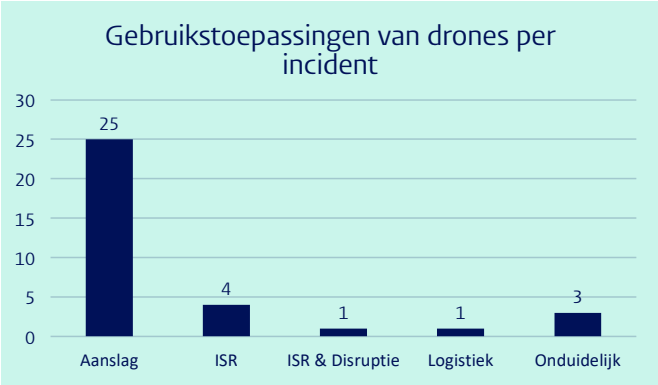
In totaal werden 34 incidenten in de periode 2010 tot en met 2025 geïdentificeerd. In elk jaar vonden incidenten plaats, met uitzondering van de jaren 2010, 2012, 2015 en 2016. Gemiddeld vonden er per jaar iets meer dan twee incidenten plaats. In zowel 2024 als 2025 vonden er acht incidenten plaats – een aanzienlijke stijging ten opzichte van voorgaande jaren. Incidenten vonden verdeeld over het hele Westen plaats, waarbij het merendeel van de incidenten (12/34) in de Verenigde Staten plaatsvond. Ook in Duitsland (4), Frankrijk (4) en het Verenigd Koninkrijk (3) vonden relatief veel incidenten plaats.



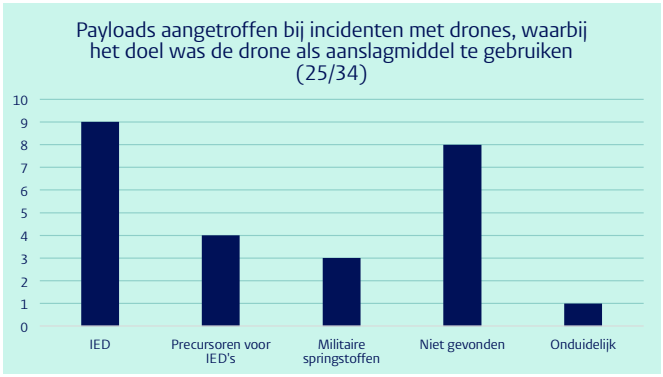
Van de 34 incidenten betroffen er 22 incidenten (65%) aanslagplannen die niet ten uitvoer kwamen. Slechts twaalf van de 34 incidenten (35%) kwamen ten uitvoer. Bij 23 van de incidenten (68%) werd daadwerkelijk een drone ingezet, of – in gevallen waarin het bij een plan bleef dat niet tot uitvoering kwam – werd tijdens een huiszoeking een drone of onderdelen daarvan aangetroffen. In 15% van de gevallen werden geen drones of onderdelen aangetroffen en betrof het dus uitsluitend een plan om drones in te zetten.

In 17% van de gevallen kon op basis van de beschikbare data niet worden vastgesteld of er drones of onderdelen daarvan aanwezig waren.

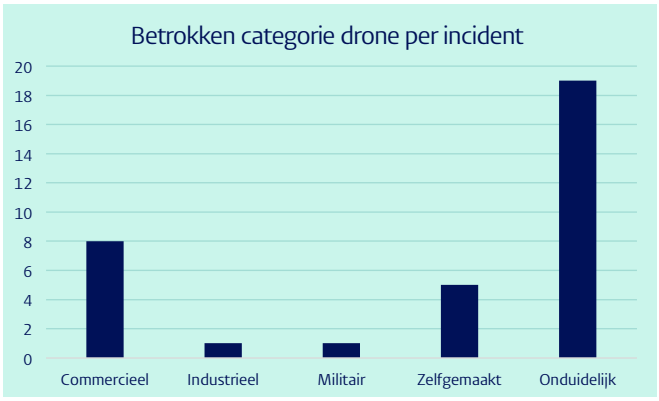
Bij drie kwart van de incidenten speelde de drone een primaire rol bij de aanslag(poging); bij het grootste deel van de incidenten uit de dataset was het doel om de drone te gebruiken als aanslagmiddel (25/34). Bij slechts vier van de incidenten werd de drone ingezet als hulpmiddel bij voorverkenning of het verzamelen van real-time intelligence tijdens een aanslag. Bij één incident werden drones als disruptiemiddel ingezet, en bij één incident werd een drone als logistiek hulpmiddel ingezet. Bij het laatstgenoemde incident werd een drone gebruikt om een vuurwapen een gevangenis in te smokkelen, om deze vervolgens te gebruiken voor een aanslag op enkele medegevangenen.



Bij het merendeel van de incidenten uit de dataverzameling waarbij het doel was om de drone als aanslagmiddel te gebruiken (25/34) was het onduidelijk (13/25) op welke wijze de payload bij het doelwit zou worden gebracht. Bij zeven van de 25 van deze incidenten was het doel om het explosief vanaf boven op het doelwit te laten vallen, terwijl bij vier drones het doel was deze in te zetten als kamikazedrones. In acht van de 28 gevallen (29%) waarin de drone (mogelijk) werd gebruikt om een payload bij een doelwit te krijgen, kon op basis van de beschikbare bronnen worden vastgesteld dat de drone was gemodificeerd met een aflevermechanisme voor de payload. Bij de 25 incidenten waarbij zeker was dat het doel was om de drone in te zetten als aanslagmiddel, werden in zestien gevallen (64%) ook daadwerkelijk explosieven of precursoren daarvoor aangetroffen. In negen gevallen werden IED's aangetroffen, in vier gevallen precursoren voor IED's, en in drie gevallen werden er militaire springstoffen aangetroffen: C4 en TNT.



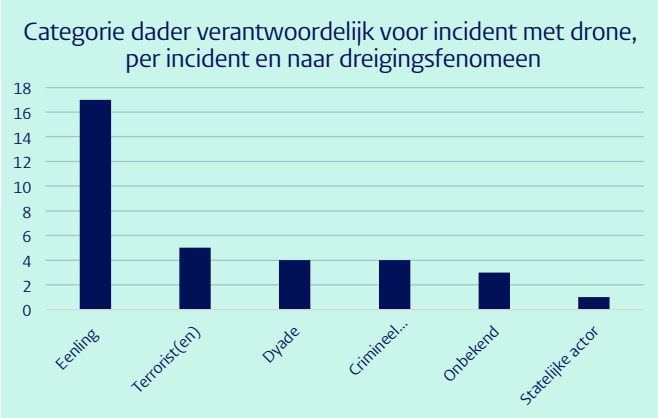
Bij de incidenten werden verschillende typen drones gebruikt, aangetroffen of beoogd om te worden ingezet. Bij het merendeel van de incidenten was het op basis van openbare bronnen echter niet mogelijk om te herleiden om wat voor type drone het ging. Bij de incidenten waarbij dit wel te herleiden was (15/34), betrof het merendeel (8/15) commerciële drones, waarna zelfgemaakte drones volgden (5/15). Van de commerciële drones betrof het merendeel drones van de producent DJI, waaronder de modellen Phantom en Mavic. Slechts één incident betrof een industriële drone (ook van DJI), en één drone – het eerste incident, uit 2011 – betrof een plan om een militair vliegtuig (een F-86 *Sabre*) om te bouwen tot een zelfsturende drone.



Bij tien van de twaalf aanslagplannen die ten uitvoer kwamen werd de drone daadwerkelijk gelanceerd, en van deze tien succesvolle lanceringen, mislukte het uiteindelijk in vier van de tien gevallen (40%) om het doel van de aanslagpoging te bereiken. In drie van de vier gevallen was de mislukte poging toe te schrijven aan een fout van de bestuurder van de drone, en in één geval werd de aanslagpoging verijdeld door de veiligheidsdiensten, die de verdachte en zijn aanslagpogingen al langer in het vizier hadden. Ook in het geval van de aanslagpogingen die nooit tot uitvoer kwamen (22/34), is het merendeel verijdeld en

werden deze in alle gevallen voorkomen dankzij de intelligencepositie van de veiligheidsdiensten. In geen enkel geval werd een dreigingsactor van tevoren gesnapt tijdens een voorverkenningspoging (door bijvoorbeeld oplettende burgers, omstanders of beveiligers rondom een doelwit). Ook werd geen enkele aanslagpoging voorkomen of ontdekt met behulp van de inzet van counter-UAS systemen, of mislukte een aanslagpoging door omgevingsfactoren (zoals slecht weer) of technische problemen met de drone.

Veruit de meeste incidenten (50%) zijn toe te kennen aan (ideologisch en niet-ideologisch gemotiveerde) eenlingen, gevolgd door terroristen (15%) en (ideologisch en niet-ideologisch gemotiveerde) dyades[1] (12%). Ook criminelen of CSV's waren verantwoordelijk voor ongeveer 12% van de incidenten, en statelijke actoren slechts voor één incident. Van één overig incident is niet bekend welk type dader er verantwoordelijk was voor het incident.



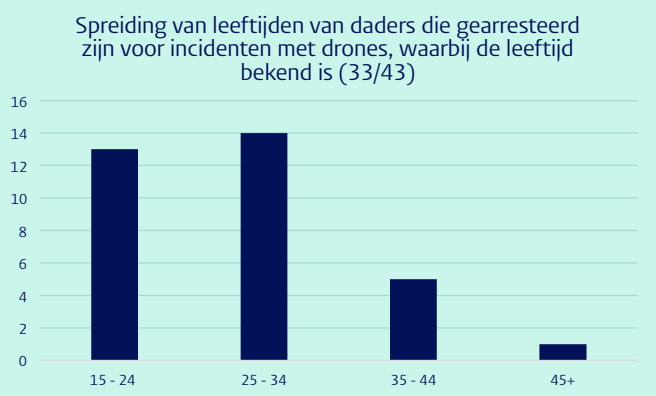
Van de incidenten die door terroristen, eenlingen of dyades (26/34) werden gepleegd, waren voor 16 incidenten daders die jihadistisch gedachtegoed aanhingen verantwoordelijk. Bij zes incidenten waren daders met rechtsextremistische motieven betrokken, en vier incidenten werden gepleegd door daders met voornamelijk persoonlijke grieven. Van de daders die lid van een terroristische groep of beweging waren, werd één incident voorbereid door leden van Hezbollah en één incident werd voorbereid door leden van Hamas.

Van de rechtsextremistische groepen met formele banden met een groep of beweging werd één gepleegd door leden van een lokale neonazigroep (ongenoemd) in Duitsland, één incident door een zelfbenoemd lid van de "Order of Nine Angles" die zijn aanslag voorbereidde met meerdere medeplegers die informanten bleken, en één incident waarbij de dader lid was van een ongenoemde rechtsextremistische groep. Onder het cohort eenlingen en dyades (21/34) was veruit het meest (14/21) jihadist, en van deze groep (14) was 64% geïnspireerd door Islamitische Staat (IS); van de overige jihadisten werden er drie geïnspireerd door Al Qaeda en bij de overige drie incidenten die gelinkt werden aan jihadisme was het niet mogelijk te achterhalen door welke groep zij zich lieten inspireren.

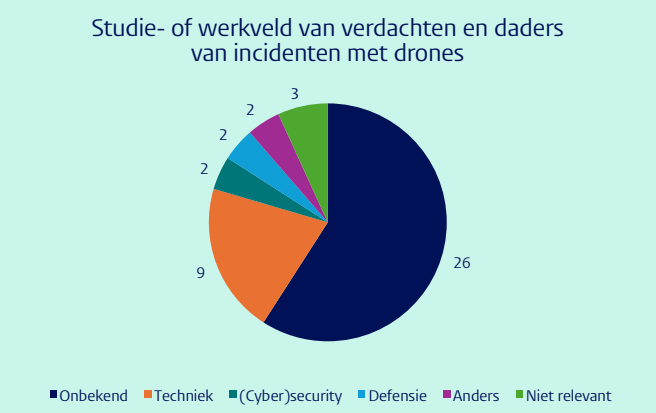
Bij vrijwel elk incident uit de dataset is er minimaal één dader of verdachte aangehouden (31/34). Bij 30 incidenten zijn in totaal 43 verdachten aangehouden. Uitzondering hierop is één incident rondom Franse gevangenissen, waarbij een onbekend aantal drones door een onbekend aantal verdachten is ingezet. Omdat het aantal verdachten bij dit incident niet te achterhalen viel is besloten deze verdachten niet mee te nemen in de uiteindelijke dataset. Van de 43 verdachten is slechts één verdachte vrouw – de echtgenote van een hoofdverdachte in een zaak, die medeplichtig wordt geacht (één van de dyades). In alle andere gevallen waren de verdachten mannen (86%) of was het geslacht van de dader niet bekend of niet herleidbaar (12%).

Van 33 van de 43 verdachten was de leeftijd (ten tijde van het incident of de arrestatie van de verdachte) te achterhalen in openbare bronnen. Van deze 33 verdachten van wie de leeftijd te achterhalen viel, is de gemiddelde leeftijd 28 jaar. De mediaan is 26 jaar oud. De jongste verdachte in het databestand is 16 jaar oud, en de oudste 58 jaar oud. Daarbij moet worden opgemerkt dat het merendeel van de verdachten waarvan de leeftijd bekend is, zich in de leeftijdscategorie 16 – 34 jaar bevindt (82%).

1 Onder de term 'dyade' worden duo's verstaan die gezamenlijk opereren, maar die – net als eenlingen – geen formele banden hebben met een bekende, bredere (terroristische) beweging of groepering. Er is ervoor gekozen deze categorie afzonderlijk te onderscheiden, omdat de beperkte empirische literatuur over dit fenomeen (Kenyon et al., 2025; O'Connor et al., 2018) erop wijst dat dit type verdachten in achtergrondkenmerken en radicaliseringsproces verschilt van bijvoorbeeld individuen die zich aansluiten bij terroristische groeperingen, en mogelijk sterker overeenkomt met eenlingen. Daarnaast zijn meerdere dyades in deze dataset niet ideologisch gemotiveerd en evenmin geaffilieerd met een bredere groep of beweging, waardoor het analytisch onlogisch zou zijn om deze actoren uitsluitend op basis van hun groepsgrootte onder de categorie 'terroristen' te scharen.

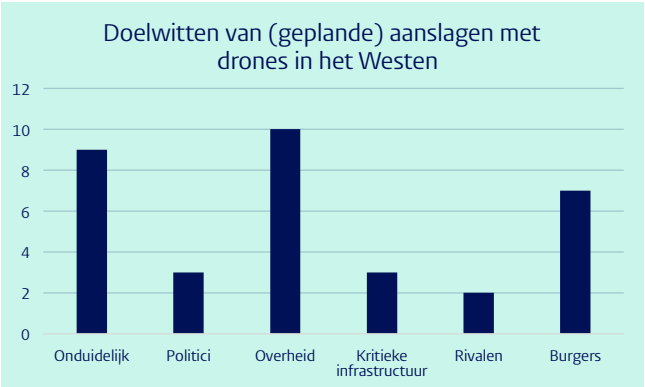


Van 28 van de verdachten was het niet mogelijk om te achterhalen wat hun hoogst behaalde niveau van onderwijs was, of welk niveau van onderwijs ze volgden tijdens hun arrestatie. Zeven verdachten deden een studie op de universiteit of hadden die afgemaakt, vijf verdachten hadden enkel de middelbare school afgemaakt, één een beroepsopleiding en één andere verdachte een *associate degree*. Van 26 verdachten was het niet mogelijk om te achterhalen in welk studie- of werkveld zij actief waren. Echter, van de verdachten waarbij dit wel viel te achterhalen (15/44), was het merendeel actief in een veld zoals techniek, (cyber) security of defensie.



In de gevallen waarbij dit te herleiden was aan de hand van de aard van de operatie zelf, of uitingen van de verdachten of daders van een incident (18/34), is achterhaald wat het doel van de inzet van de drone was. In al deze gevallen was het doel van het gebruik van de drone om beveiligingsmaatregelen rondom een *hard target* (een beveiligd doelwit) te overkomen. In 14 gevallen was het doel om een aanslag te plegen op een hard target, in twee gevallen werd er een voorverkenning rondom een hard target met de drone uitgevoerd (met de intentie om detectie als gevolg van een andere vorm van voorverkenning te voorkomen), en in twee gevallen werden drones gebruikt om real-time intelligence rondom beveiligde doelwitten te verzamelen tijdens de uitvoering van een aanslag. In vier van de gevallen waarbij het doel was om een hard target aan te vallen, bespraken de daders ook de gewenste maatschappelijke impact die een aanslag met een drone op een specifiek (beveiligd) doelwit zou genereren, waarbij in deze gevallen het doelwit de Belgische premier, de Amerikaanse president, een militaire basis en het Pentagon/het Capitool betroffen. De redenen om een drone in te zetten lijken in die zin multidimensionaal, en het is mogelijk dat andere daders ook voor een drone kozen vanwege de veronderstelde psychologische en maatschappelijke impact.

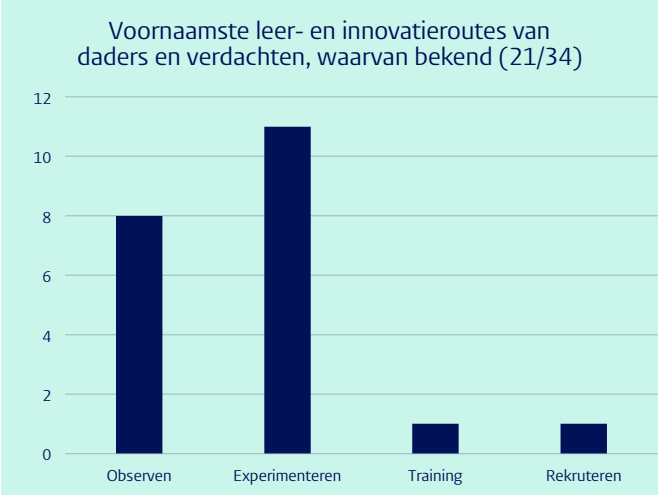
De aantrekkingskracht van drones als middel om hard targets te bereiken blijkt ook uit de verdeling van het type doelwit bij de verschillende incidenten. Bij dertien van de 34 incidenten waren overheidsgebouwen, militaire bases, overheidsfunctionarissen of politici het doelwit, en bij drie incidenten kritieke infrastructuur. Slechts twee incidenten waren gericht op rivalen en zeven op burgers.



Van twaalf van de 34 incidenten (35%) was op basis van openbare bronnen met zekerheid te achterhalen dat de verdachte(n) of dader(s) van tevoren (meermaals) hebben geoefend met het besturen van de drone. Ten slotte zijn er verschillende leer- en innovatieroutes te identificeren in de dataset.

Van het deel van de incidenten waarbij de leer- of innovatieroute van de dader bij het gebruik van een drone bekend is (21/34), experimenteerde het merendeel zelf met het bouwen en vliegen met een drone (52%). Daarna volgde een groot deel van de daders dat via het observeren in openbare bronnen (38%) met drones aan de slag is gegaan. Hierbij moet worden benoemd dat het label "observeren" een bepaalde mate van passiviteit veronderstelt. Echter, een groot deel van deze daders consumeerde niet uitsluitend instructies over het bouwen van drones, maar produceerden zelf ook handleidingen en instructies. In één geval vroeg een dader (online) direct om hulp van een expert in het bouwen van drones van Islamitische Staat in Irak en Syrië (*training*), en in een ander geval huurde een groep rechtsextremisten een burger met specialistische kennis in (*rekruteren*) om een drone en explosief voor hen te bouwen.

Ook bij deze datapunten is enige nuance met betrekking tot de categoriale codering van de dataset geboden. Immers, het feit dat sommige van de 'observeerders' die actief zijn in online netwerken waar informatie werd gedeeld zelf ook informatie en instructies produceerden en deelden, veronderstelt ook enige mate van handelingen die onder het label 'experimenteren' zouden kunnen vallen. Ook is het aannemelijk dat 'experimenteerders' uit de dataset niet geheel op eigen houtje experimenteerden, maar actief hebben gezocht naar online instructies, maar dat deze informatie niet op basis van openbare bronnen te achterhalen is. Ook moet worden opgemerkt dat vrijwel alle 'observeerders' die actief waren in online netwerken jihadistische eenlingen betroffen, van wie een groot deel geïnspireerd was door Islamitische Staat. In twee gevallen betroffen het rechtsextremistische eenlingen die actief waren in online netwerken.



Discussie

Deze sectie van de studie beoogde systematisch in kaart te brengen hoe verschillende dreigingsactoren sinds 2010 drones hebben ingezet in Westerse landen. De resultaten laten zien dat het gebruik van drones door dreigingsactoren in het Westen in absolute zin nog beperkt is (34 incidenten in vijftien jaar), maar dat er tegelijkertijd duidelijke aanwijzingen zijn voor een recente, constante toename in het aantal incidenten. In 2024 en 2025 werd een opvallende stijging zichtbaar (beide jaren acht incidenten), terwijl in de eerdere jaren (tot 2018) de incidentfrequentie laag of nihil bleef.

Dit correspondeert grofweg met de data die Haugstvedt (2024) rapporteert in zijn dataset van geslaagde droneaanslagen wereldwijd, waar ook een fluctuerende maar tamelijk constante stijging van incidenten tussen 2018 en 2023 te zien is. Waar de vroege experimenten met drones lange tijd vooral geassocieerd werden met conflictgebieden en enkele "innovatoren" die daar actief zijn, zoals ISIS en verschillende Mexicaanse kartels, suggereren de bevindingen dat dronegebruik als modus operandi in het Westen mogelijk opschuift richting een bredere groep potentiële gebruikers. Hoewel deze stijging eerder lineair dan exponentieel lijkt, sluit deze ontwikkeling aan bij de verwachting dat de zichtbaarheid van succesvolle toepassingen en verdere proliferatie van technologie dronegebruik door kwaadwillende actoren zal versnellen (Doctor, 2025; Rogers, 1983).

Tegelijkertijd relativeert de dataset het schrikbeeld dat drones in het Westen op ieder moment op grote schaal en succesvol kunnen worden ingezet door dreigingsactoren. Een kernbevinding uit de data is dat het merendeel van de geïdentificeerde incidenten plannen betrof die nooit ten uitvoer kwamen (65%). En van de twaalf van de 34 incidenten (35%) die ten uitvoer kwamen mislukte een substantieel deel (4/12) alsnog door fouten van de dader of interventie van de veiligheidsdiensten. Dit wijst op een paradox die ook in de probleemstelling centraal stond: ondanks de steeds grotere beschikbaarheid van drones en kennis, blijft succesvolle inzet voor een aanslag (in het Westen) vooralsnog relatief schaars. De verklaring hiervoor lijkt in belangrijke mate te liggen in de combinatie van (a) de operationele complexiteit van drone-aanslagen en (b) het beperkte relatieve voordeel ten opzichte van eenvoudiger alternatieven in de Westerse context.

De resultaten laten zien dat – hoewel veel plannen verijdeld zijn en veel gelanceerde plots uiteindelijk ook falen – de aanslagplannen zelf niet triviaal zijn. Bij het merendeel van de incidenten, inclusief de pogingen tot inzet van een drone, werden daadwerkelijk drones gevonden. Ook werd bij een aanzienlijk deel van de incidenten waarbij het doel had een drone als aanslagmiddel te gebruiken explosieven of precursoren aangetroffen. Een aanzienlijk deel van de plannen bevond zich dus in een gevorderd stadium en betrof niet louter de hypothetische inzet van een drone.

Echter ligt de drempel voor de succesvolle inzet van een drone bij een aanslag niet uitsluitend bij het kunnen vliegen met een drone, maar in het kunnen bedenken en uitvoeren van een integrale aanvalscyclus met een drone. Daarbij moeten het gebruik van een payload, ontstekings- en aflevermechanisme, *operational security* van de dreigingsactor tijdens voorbereiding, en de uitvoering van de aanslag succesvol bij elkaar komen (Doctor, 2025). Deze complexiteit wordt mede zichtbaar in het grote aandeel verijdelde plannen in de dataset: de aanschaf of ontwikkeling van de drone, het eventuele aanpassen van de drone, het oefenen met vliegen, en de verwerving van explosieven zijn allemaal stappen die succesvol doorlopen moeten worden. Waarschijnlijk leidt dit tot een relatief lange incubatieperiode van een plot, waardoor mogelijk de pakkans wordt vergroot of de aandacht, zorgvuldigheid of motivatie van een actor kan afnemen, en er meer risico op operationele fouten ontstaat.

In de Westerse context komt daar een extra belemmerende factor bij: het verwerven van explosieven of precursoren is gereguleerd en daardoor extra risicovol (Doctor, 2025), waardoor de bottleneck van de succesvolle inzet van een drone bij een aanslag zich deels verplaatst van de drone naar het verkrijgen van de payload. Het merendeel van de aangetroffen explosieven betrof waarschijnlijk om die reden ook geïmproviseerde explosieven (IED's). De data illustreert in die zin ook waarom het relatieve voordeel van drones voor veel actoren in de Westerse context mogelijk beperkter is dan in de conflictgebieden waar ze wel wijdverspreid worden toegepast: waar dreigingsactoren die een aanslag willen plegen met een drone in oorlogssituaties kunnen rekenen op beschikbare munitie en andere gunstige omgevingscondities, vereist een drone-aanslag in het Westen een vrij complexe set aan vaardigheden en omstandigheden die de aantrekkelijkheid van alternatieven (vuurwapens, voertuigen, messen) vergroot (Doctor, 2025; Nationaal Coördinator Terrorismebestrijding- en Veiligheid, 2024).

Een andere kernbevinding betreft de verdeling van de verantwoordelijke actoren. De oververtegenwoordiging van jihadistische daders (waaronder voornamelijk eenlingen) in deze dataset – en de ogenschijnlijke doorwerking van inspiratie door Islamitische Staat – past bij Rogers' (1983) karakteristiek van observeerbaarheid. IS fungeert als pionier in het populariseren van dronegebruik en produceert propaganda die de effectiviteit van drone-aanslagen benadrukt (Bouhlaoui, 2025). Dat effect lijkt in de Westerse context voort te werken via online netwerken, waarin niet alleen passieve consumptie van zulke propaganda plaatsvindt, maar ook actieve productie en verspreiding van instructies voor het gebruik van drones voor een aanslag.

De waarnemingen uit de dataset sluiten ook aan bij de verwachting dat vooral actoren met beperkte organisatorische capaciteit relatief vaak naar drones grijpen: eenlingen en dyades waren verantwoordelijk voor het grootste aandeel van de incidenten. Dit lijkt op het eerste gezicht contra-intuïtief, omdat drone-aanslagen complex lijken. Een plausibele interpretatie is dat drones voor deze actoren vooral aantrekkelijk zijn vanwege symboliek en verwachte media-impact en de compatibiliteit met het streven naar maatschappelijke ontwrichting (Bouhlaoui, 2025). Ook zijn drones voor daders met minder operationele slagkracht, zoals dyades en eenlingen, een manier om hard targets te bereiken die met andere aanslagmethoden minder makkelijk te bereiken zijn. De resultaten ondersteunen die lezing: waar het motief te herleiden was, was

De resultaten laten zien dat het gebruik van drones door dreigingsactoren in het Westen in absolute zin nog beperkt is. Tegelijkertijd is er recent een constante toename in het aantal incidenten.

het doel in alle gevallen gerelateerd aan het overkomen van beveiligingsmaatregelen rond hard targets.

Ook de empirische studie van Haugstvedt (2024), van aanslagen met drones wereldwijd, laat zien dat hard targets een geliefd doelwit voor drone-aanslagen zijn. Hij rapporteert dat 71,4% van de aanslagen uit zijn dataset gericht zijn op hard targets. Dit wijst op de veronderstelde operationele voordelen die dreigingsactoren zien in het gebruik van drones, vooral in relatie tot hard targets. Ook is het mogelijk dat daders zich beperken tot aanslagen op specifieke hard targets, omdat met name commerciële drones beperkt zijn in het dragen van grote, zware payloads die een groot aantal slachtoffers of een grote schaderadius kunnen veroorzaken. Drones lijken zich dus eerder te lenen voor aanslagen op specifieke doelwitten, zoals personen, waarbij een explosief dat een beperkt verwoestend effect heeft voldoende is om het doelwit uit te schakelen. In dat opzicht blijven andere aanslagmiddelen, zoals explosieven in een rugtas of voertuig, of aanslagen met vuurwapens, effectievere alternatieven voor het plegen van grote aanslagen op soft targets (Doctor, 2025).

De wijze waarop incidenten met drones worden verijdeld is ook opvallend. De dataset suggereert dat vrijwel alle verijdeling van aanslagplannen plaatsvond als gevolg van vroegtijdige interventie door de veiligheidsdiensten, en niet vanwege detectie door counter-UAS-systemen of door oplettendheid van beveiligers en omstanders tijdens bijvoorbeeld een voorverkenning of aanslagpoging. Op het eerste gezicht kan dit worden geïnterpreteerd als aanwijzing dat counterdronecapaciteiten in de onderzochte periode beperkt hebben bijgedragen aan de preventie van droneaanslagen. Anderzijds vereist deze conclusie terughoudendheid, omdat hier de preventieparadox speelt: succesvolle afschrikking van een dreigingsactor die een plan had een aanslag met een drone te plegen als gevolg van de aanwezigheid van zulke systemen is per definitie nauwelijks zichtbaar in open bronnen. Als counter-UAS heeft geleid tot de mitigatie van een incident zonder dat dat gepaard is gegaan met brede publiciteit, is zo'n incident in deze dataset niet vertegenwoordigt. Desondanks is relevant dat bij geen enkel geïdentificeerd incident duidelijk werd dat een droneplot primair mislukte door interceptie van de drone of door weers- en omgevingsfactoren. Dat suggereert dat – bij de incidenten die geïdentificeerd zijn in dit openbronnenonderzoek – opsporings- en inlichtingenposities en menselijke fouten dominanter waren dan counterdronecapaciteiten als verklarende factor voor het mislukken van aanslagpogingen.

Hard targets lijken een geliefd doelwit voor aanslagen met drones.

Opvallend is ook wat nauwelijks voorkomt: criminele samenwerkingsverbanden en statelijke actoren lijken tot dusver nauwelijks verantwoordelijk te zijn voor aanslag(plannen) met drones in het Westen. Een mogelijke verklaring hiervoor is de relatief hoge mate van attributie bij incidenten met drones, waarbij ze daadwerkelijk worden ingezet voor aanslag(plannen). In de literatuur wordt verondersteld dat de veronderstelde beperkte attributie een sterke beweegreden is voor actoren om drones in te zetten (Bouhlaoui, 2025; Veilleux-Lepage & Archambault, 2022). Echter, zoals Doctor (2025) in zijn conceptuele bijdrage betoogt, lijken de data uit deze studie er op te wijzen dat het gebruik van een drone het risico soms juist vergroot, en dat een dader zijn *operational security* makkelijk kan compromitteren. Bij een groot deel van de incidenten in de dataset van deze studie slaagden autoriteiten erin de dader(s) te identificeren. Daarbij moet worden benadrukt dat het merendeel van de incidenten in deze dataset betrekking heeft op verijdelde aanslagplannen, wat logischerwijs leidt tot een selectiebias richting incidenten die zijn mislukt en daardoor relatief eenvoudig te attribueren zijn. Tegelijkertijd geldt dat ook een substantieel deel van de aanslagplannen die wel tot uitvoering kwamen ook succesvol kon worden geattribueerd aan een dader.

Deze bevindingen zijn relevant voor het afwegingskader van actoren waarvoor *plausible deniability* of organisatorische levensvatbaarheid meer centraal staat. Voor statelijke actoren – maar mogelijk ook voor criminele organisaties die onder de radar willen blijven – kan de relatief hoge attributiekans een remmende werking hebben op de keuze voor de inzet van een drone, zeker als een drone-incident met dodelijke afloop extra repressie en opsporingsaandacht uitlokt. Dit kan mede verklaren waarom statelijke actoren in deze dataset nauwelijks zichtbaar zijn in het domein van drone-aanslagen met een duidelijke gewelds-intentie, ondanks het wijdverspreide gebruik van bijvoorbeeld Rusland in Europa, voor zogenaamde

grey zone-tactieken, waarbij ze inlichtingen verzamelen en vijandige staten intimideren, maar enige mate van ontkenning voor zo'n incident kunnen aanhouden (Favia et al., 2025). Het suggereert dat voor sommige actoren het strategische nadeel (aandacht, repressie of diplomatieke problemen) zwaarder weegt dan het (mogelijke) operationele voordeel.

Complexe vormen van dronegebruik, zoals *combined arms*-toepassingen waarbij drones geïntegreerd worden in gecoördineerde aanvallen, zijn in de dataset ook nagenoeg afwezig. Slechts twee incidenten wijzen op dergelijke meer geavanceerde toepassingen; beide betroffen twee van de drie incidenten die toe te rekenen zijn aan criminele organisaties. Dit ondersteunt het idee uit de literatuur dat dergelijke toepassingen aanzienlijk meer middelen, coördinatie en organisatorisch lerend vermogen vereisen dan de meeste actoren bezitten. In die zin is het beperkte voorkomen van complexe toepassingen ook consistent met de theoretische verwachting dat complexiteit en organisatorische capaciteit sterk samenhangen met het type dronegebruik dat voor bepaalde actoren haalbaar is (Haugstvedt, 2021; Rogers, 1983), zoals bijvoorbeeld voor de eenlingen die de dataset van dit onderzoek domineren.

Ten slotte bieden de sociaaldemografische patronen van de daders uit de dataset inzicht in welke individuen geneigd lijken een aanslag met een drone te plegen, dan wel een poging daartoe te ondernemen. De concentratie van daders in de leeftijdscategorie van de late twintigers tot begin dertigers suggereert dat de inzet van drones mogelijk samenhangt met factoren als geduld, technische vaardigheden en de beschikbaarheid van financiële middelen. Het verwerven, aanpassen en testen van een drone, evenals het verkrijgen van (precursoren voor) een explosief, vergt tijd, planning en geduld, en sluit daarmee mogelijk minder goed aan bij de handelingsrepertoires van zeer jonge daders. Voor jongere daders kan het relatief eenvoudiger zijn om terug te grijpen op alternatieve aanvalsmiddelen die minder voorbereiding vereisen en minder opvallen, zoals vuur- of steekwapens. Tegelijkertijd lijkt de technologie ook minder aantrekkelijk voor aanzienlijk oudere daders. Een mogelijke verklaring is dat dit cohort niet is opgegroeid met nieuwe, digitale technologieën, game-interfaces en controllers zoals joysticks, wat de drempel om drones te gebruiken kan verhogen. In combinatie met mogelijke beperkingen in technische vaardigheden en leercapaciteit kan dit ertoe bijdragen dat drones vooral worden overwogen door daders in een specifieke levensfase, waarin zowel vertrouwdheid met nieuwe technologieën als praktische middelen aanwezig zijn. Echter, de proliferatie van drones zal ervoor zorgen dat in de toekomst, meer personen – van jong tot oud – kundig zullen zijn in het gebruik van drones (Doctor, 2025).

Ten slotte suggereren de beschikbare data een hogere vertegenwoordiging van personen met specifieke vaardigheden en interesses onder de geïdentificeerde daders en verdachten. Hoewel het bij het merendeel van de verdachten niet mogelijk was dit te achterhalen, kwam een opvallend aandeel daders en verdachten uit technische, (cyber)security- of defensiegerelateerde achtergronden. Dit kan twee verklaringen hebben: enerzijds voelen daders met deze achtergrond zich mogelijk aangetrokken tot drones omdat zij beschikken over de interesse en expertise om drones, aflevermechanismen en payloads effectief te ontwikkelen. Anderzijds kan het zijn dat juist plannen van deze daders een vergevorderd stadium bereikten, terwijl minder competente daders hun plannen met drones voortijdig hebben gestaakt vanwege de complexiteit, en daardoor buiten beeld blijven. Deze resultaten moeten bovendien niet worden geïnterpreteerd als een aanwijzing dat er een specifiek profiel is van een mogelijke aanslagpleger met een interesse in drones. De vertegenwoordiging van daders met een dergelijke achtergrond is eerder relevant als extra indicatie dat de *barrier-to-entry* voor dronegebruik niet uitsluitend wordt bepaald door toegang tot middelen, maar mogelijk ook door kennis en praktische vaardigheden.

Eenlingen en terroristische organisaties zijn grotendeels verantwoordelijk voor incidenten met drones.

Beperkingen

Deze studie kent een aantal beperkingen die in acht moeten worden genomen bij de interpretatie van de resultaten. Ten eerste is de dataset samengesteld op basis van openbronnenonderzoek naar (verijdelde) aanslagen. De studie analyseerde alle geregistreerde incidenten die voldeden aan de inclusiecriteria binnen

de onderzochte periode (n = 34). Hoewel deze dataset daarmee een overzicht van *waargenomen* incidenten vormt, moet de interpretatie van de resultaten met voorzichtigheid gebeuren. Incidenten met drones zijn maatschappelijk en bestuurlijk gevoelig, en worden per definitie gekenmerkt door beperkte transparantie wat betreft details, veelal als gevolg van onvolledige mediaberichtgeving en de selectieve openbaarmaking van details over de incidenten door bijvoorbeeld het openbaar ministerie of de politie in het desbetreffende land. Hierdoor is het mogelijk dat er incidenten hebben plaatsgevonden die nooit bekend zijn geworden en dus ook niet in deze dataset zijn opgenomen. De resultaten moeten dan ook worden gelezen als een empirisch onderbouwde analyse van *gedetecteerde* en *gerapporteerde* incidenten, en niet als een compleet overzicht van *alle* incidenten.

Ook vertaalt de bovengenoemde beperking zich in een beperkte datakwaliteit; een relatief hoog aandeel variabelen in de data is als 'onduidelijk' of 'onbekend' is gecodeerd. Hierbij is het tegelijkertijd belangrijk om te benoemen dat de ontbrekende informatie of variabelen niet willekeurig lijkt te zijn verdeeld. Informatie die relevant zijn voor variabelen zoals locatie van het incident, dadercategorie, motivatie, uitkomst van het incident en informatie over de verijdeling door de veiligheidsdiensten is bij het merendeel van de geïdentificeerde incidenten wel beschikbaar. De ontbrekende data concentreren zich daarentegen op vrij gedetailleerde tactische of gevoelige aspecten, hetgeen plausibel samenhangt met (bewuste) afscherming van zulke informatie door opsporings- en veiligheidsdiensten of met het feit dat veel aanslagplannen zich in een vroeg stadium bevonden en de betreffende aspecten nog niet bekend waren.

Samenvattend moet de lezer in acht nemen dat de bevindingen dus primair betrekking hebben op gedocumenteerde gebeurtenissen. Als gevolg van de relatief kleine omvang van de dataset, evenals de kwaliteit van de data, moet worden benadrukt dat de interpretaties uit de beschrijvende statistiek, zoals percentages, door de lezer met nuance dienen te worden geïnterpreteerd en primair als indicatief moeten worden beschouwd. Desondanks bieden de analyses waardevolle inzichten in patronen en kenmerken binnen de geregistreerde incidenten, die relevant zijn voor begrip van incidenten met drones, en welke – ondersteund door meer data – in de toekomst kunnen leiden tot hypothesevorming. Deze studie moet dus vooral worden gezien als verkennend, en is zodoende een uitnodiging naar onderzoekers om in de toekomst incidenten bij te blijven houden en (eventueel met behulp van het (door)ontwikkelde codeboek uit deze studie) te blijven analyseren.

Het voorkomen van aanslagen met drones lijkt in belangrijke mate afhankelijk van een sterke intelligencepositie van de politie en veiligheidsdiensten, naast investeringen in technische counterdronecapaciteiten.

Praktijkaanbevelingen

De bevindingen van deze studie laten zien dat met name eenlingen, dyades en terroristen tot dusver verantwoordelijk zijn voor aanslag(plannen) in het Westen waarbij drones een rol spelen. Hoewel de studie zich baseert op een relatief kleine dataset van gerapporteerde incidenten (n = 34), benadrukt dit dat politie en veiligheidsdiensten rekening moeten houden met de aantrekkingskracht van dit type aanslagen voor eenlingen en kleine samenwerkingsverbanden.

Het merendeel van de aanslagplannen werd verijdeld als gevolg van de intelligencepositie van de veiligheidsdiensten, en niet door de inzet van counter-UAS-capaciteiten. Het voorkomen van aanslagen met drones lijkt dus in belangrijke mate afhankelijk van een sterke intelligencepositie, naast investeringen in technische counterdronemaatregelen.

Op basis van de data kan intelligence zich bij vroegtijdige detectie met name richten op twee aspecten. Ten eerste kunnen inlichtingendiensten zich richten op (extremistische) online netwerken waarin de ontwikkeling en inzet van drones voor aanslagen, evenals de verwerving en ontwikkeling van explosieven voor dergelijke aanslagen, worden besproken.

Het merendeel van de eenlingen, dyades en terroristen in deze dataset liet zich inspireren door Islamitische Staat – die aanslagen met drones in online netwerken propageren – en besprak plannen, technische ontwerpen of consumeerde of produceerde instructies over drones in dergelijke netwerken. Ook een substantieel deel van de rechtsextremistische daders deed dit. Kortom, online netwerken lijken een belangrijk aanknopingspunt voor vroegtijdige signalering.

Ten tweede kan vroegtijdige detectie zich blijven richten op potentiële daders die payloads proberen te verkrijgen; en in het bijzonder (precursoren voor) IED's. Hoewel de toegang tot drones zelf laagdrempelig is, vormt het verwerven van explosieven en precursoren waarschijnlijk een bottleneck voor potentiële daders. Bestaande maatregelen rondom controle op explosieven en precursoren hebben daardoor mogelijk een indirect maar substantieel preventief effect, en vergroten mogelijk de pakkans, mede door de verlenging van de incubatietijd van aanslagplannen.

Ten derde kan het – op basis van theoretische inzichten – wenselijk zijn voorbereid te zijn op de gevolgbestrijding van de (maatschappelijke) impact van drone-aanslagen. De data uit deze studie suggereren dat propaganda een aanzuigende werking kan hebben op het plegen van aanslagen met drones. Daarnaast is de zichtbaarheid van succesvolle drone-aanslagen de afgelopen jaren toegenomen, bijvoorbeeld door berichtgeving over het slagveld in Oekraïne. Hierdoor bestaat de kans dat een succesvolle en ingrijpende drone-aanslag – met name wanneer deze gepaard gaat met videobeelden en bijvoorbeeld gericht is op een hoogwaardig doelwit, zoals een bekende politicus of bestuurder – breed wordt uitgemeten in de media en veelvuldig wordt gedeeld en besproken in besloten online kanalen waar kwaadwillende actoren actief zijn. Het is voorstelbaar dat zo'n incident grote maatschappelijke onrust zou veroorzaken en tegelijkertijd een aanjagend effect zou hebben op andere potentiële daders. Verschillende auteurs betogen dat de verspreiding van drones in andere contexten mede het gevolg is van dergelijke vormen van zichtbaarheid en diffusie (Bouhlaoui, 2025; Doctor, 2025).

Politie en veiligheidsdiensten kunnen zich bij vroegtijdige detectie om drone-aanslagen te voorkomen richten op twee aspecten: het monitoren van online netwerken waar aanslagplannen met drones worden besproken, en de aanpak van aanslagmiddelen zoals (precursoren voor) explosieven voortzetten.

Ten slotte benadrukken de resultaten het belang van aandacht voor hard targets. Waar motieven konden worden vastgesteld, richtten bijna alle plannen zich op het overkomen van beveiligingsmaatregelen rond (zwaar) beveiligde doelwitten of het voorkomen van detectie in de voorbereidende fase. Dit suggereert dat drones vooral worden gezien als middel om toegang te verkrijgen tot moeilijk bereikbare doelwitten, en minder als instrument voor het creëren van veel slachtoffers of schade bij soft targets. Voor professionals betekent dit dat dreigingsinschattingen rond hard targets (en specifiek personen) expliciet rekening moeten houden met drone-gerelateerde risico's, en dat signalen van mogelijke voorverkenning met drones rondom dit soort doelwitten serieus moeten worden genomen.

Verder onderzoek

Wat betreft toekomstig onderzoek benadrukken de resultaten de noodzaak van longitudinaal onderzoek naar de ontwikkeling van dronegebruik door dreigingsactoren in het Westen. De waargenomen toename in incidenten in recente jaren roept vragen op over de mate waarin deze trend structureel is, en hoe deze zich verhoudt tot de verdere proliferatie van het gebruik van drones in reguliere sectoren, en bijvoorbeeld de lange termijn-effecten van de oorlog in Oekraïne op de kennis en middelen die als gevolg van de oorlog beschikbaar worden voor kwaadwillende actoren.

Toegang tot gesloten bronnen en bredere samenwerking met de politie en veiligheidsdiensten zou hierbij kunnen helpen: de beperkte omvang van deze studie zou kunnen worden uitgebreid met data over daders die vroegtijdig zijn gedetecteerd door politie- en veiligheidsdiensten, of worden onderschept door counter-UAS systemen, maar waarover geen openbare gegevens beschikbaar zijn, evenals andere incidenten die nooit de publiciteit hebben gehaald. Deze 'onzichtbare' incidenten bleven buiten de scope van het huidige onderzoek, terwijl data over deze incidenten behulpzaam zijn voor beter begrip van de dreiging van drones. Met dergelijke data zouden de trends uit deze studie verder kunnen worden onderzocht.

Een aanvullende aanbeveling betreft het onderzoeken van online netwerken waarin drones en mogelijke aanslagtoepassingen met drones worden besproken. De bevindingen uit deze studie suggereren dat dergelijke netwerken niet alleen fungeren als bron van (passieve) inspiratie, maar ook als ruimte waarin plannen, ontwerpen en ervaringen door potentiële daders worden gedeeld. Het onderzoeken van deze netwerken kan bijdragen aan kennis over de wijze waarop dit soort plannen worden besproken, inzicht bieden in leer- en innovatieroutes van daders, en inzage bieden in bijvoorbeeld de netwerkstructuur rondom personen die eigen plannen en instructies delen in dit soort netwerken.

Tot slot is het wenselijk om de hier ontwikkelde dataset en het codeboek in de toekomst te blijven uitbreiden (bijvoorbeeld met de inzichten van experts) en actualiseren, zodat veranderingen in actortypen en operationele details van aanslagen of plannen met drones uitgebreider en systematisch kunnen worden gevolgd. Daarmee kan deze verkennende studie dienen als basis voor verdere hypothesevorming en cumulatieve kennisopbouw over dronegebruik door dreigingsactoren in het Westen.

De waargenomen toename van (gepoogde) aanslagen met drones in recente jaren benadrukken de noodzaak van longitudinaal onderzoek naar de ontwikkeling van dronegebruik door dreigingsactoren in het Westen.

Conclusie

In dit rapport werd het spanningsveld tussen de vermeende dreiging van drones als aanslagmiddel en de beperkte daadwerkelijke inzet ervan door dreigingsactoren in Westerse landen onderzocht. Door theorie over innovatie-adoptie en de bestaande literatuur over dronegebruik door kwaadwillende actoren te combineren met een systematische empirische inventarisatie van incidenten tussen 2010 en 2025, is beoogd beter te begrijpen waarom drones ondanks hun beschikbaarheid en zichtbaarheid vooralsnog slechts beperkt worden ingezet voor aanslagen.

De empirische bevindingen laten zien dat het gebruik van drones door dreigingsactoren in het Westen beperkt blijft. In vijftien jaar werden 34 incidenten geïdentificeerd, waarvan het merendeel aanslagplannen betrof die nooit tot uitvoering kwamen. Tegelijkertijd wijst de recente toename van incidenten in 2024 en 2025 erop dat het gebruik van drones voor aanslagen in het Westen mogelijk in populariteit toeneemt en blijvend aandacht verdient, en op fenomeenniveau dient te worden gemonitord. Ook blijkt uit de data dat een aanzienlijk deel van de plannen zich in een vergevorderd stadium bevond, wat benadrukt dat de intentie en bereidheid tot innovatie onder verschillende dreigingsactoren aanwezig is.

De tot nu toe beperkte inzet van drones voor aanslagen laat zich vooral verklaren door de combinatie van operationele complexiteit en een relatief beperkt voordeel ten opzichte van eenvoudiger alternatieven. Hoewel drones laagdrempelig beschikbaar zijn en specifieke tactische voordelen bieden, vereist de succesvolle inzet van een drone bij een aanslag een keten van onderling afhankelijke, risicovolle en tijdsintensieve stappen. Dit betreft onder meer het verwerven en aanpassen van een drone, het ontwikkelen of verkrijgen van een geschikte payload (vaak geïmproviseerde explosieven), de uitvoering zelf en het waarborgen van de eigen het *operational security* tijdens dit hele proces. Deze vereisten verlengen de incubatietijd van aanslagplannen en vergroten zowel de kans op detectie door veiligheidsdiensten als het risico op operationele fouten. In de Westerse context wordt deze complexiteit versterkt door gereguleerde toegang tot explosieven en precursoren, waardoor de bottleneck voor het plegen van een succesvolle aanslag zich lijkt te verplaatsen naar het vervaardigen van een payload. Dat specifieke kennis en vaardigheden hierin een rol spelen, blijkt ook uit de achtergrond van betrokkenen: voor zover bekend hadden veel daders uit de onderzochte dataset een achtergrond in techniek, defensie of (cyber)security.

Het in dit rapport ontwikkelde theoretische afwegingskader duidt deze dynamiek en plaatst deze in bredere context. Door inzichten uit innovatietheorie te combineren met empirische bevindingen, wordt duidelijk waarom drones met name aantrekkelijk zijn voor eenlingen en kleine samenwerkingsverbanden met beperkte organisatorische capaciteit. Voor deze actoren bieden drones operationele voordelen, zoals het bereiken van hard targets en het omzeilen van fysieke beveiliging. Tegelijkertijd bieden de bevindingen concrete aanknopingspunten voor beleid en praktijk. Dat de meeste aanslagplannen vroegtijdig worden verijdeld op basis van inlichtingenposities – en niet via technische counter-UAS-interventies – benadrukt het belang van blijvende investeringen in monitoring van online netwerken en risicovolle individuen, evenals in signalering van pogingen tot aanschaf van drones, onderdelen en explosieve of precursoren door dergelijke individuen. De aantrekkelijkheid van drones staat bovendien niet op zichzelf, maar wordt mede gevormd door contextuele factoren zoals technologische diffusie, online propaganda van terroristische groeperingen en de toenemende zichtbaarheid van dronegebruik in andere domeinen, die gezamenlijk de gepercipieerde effectiviteit en haalbaarheid van droneaanslagen beïnvloeden.

Samenvattend bevindt de dreiging van aanslagen met drones in het Westen zich momenteel op het snijvlak tussen mogelijkheid en realiteit. Drones vormen een reëel, maar vooralsnog beperkt en contextafhankelijk risico. Een effectieve dreigingsinschatting van dit fenomeen vraagt daarom om een ietwat nuchtere benadering: alertheid op specifieke toepassingsscenario's en actortypen die mogelijk gebruik maken van drones, zonder geleid te worden door alarmisme en angstscenario's. Het combineren van empirische data met een expliciet afwegings- en analysekader, zoals deze studie beoogde, biedt hierbij hopelijk een basis voor verdere monitoring op fenomeenniveau, evenals de ontwikkeling van beleid dat beoogt aanslagen met drones in het Westen te voorkomen en de mogelijke maatschappelijke gevolgen van zo'n aanslag te bestrijden.

Appendix A: Codeboek voor empirische studie

Variabele	Beschrijving	Codering
Incident en context		
IncidentDate	Datum vant, arrestatie of rapportage	DD-MM-||||
IncidentCountry	Land van het incident	Tekst
IncidentLoc	Stad/regio van incident of arrestatie	Tekst
Drone en payload		
DroneFound	Drone of onderdelen aangetroffen	Ja / Nee / Gepland / Onbekend
DroneApplication	Functie van de drone	ISR / Logistiek / Disruptie / Aanslag
DroneRole	Rol van de drone in het aanslagplan	Primair / Ondersteunend
PayloadFound	Payload aangetroffen	Ja / Nee / Onbekend
PayloadDescription	Type payload	IED / Precursor / Militaire springstoffen / Anders / Onbekend
PayloadDelivery	Afleverwijze payload	Pilot-to-Target / Drop / Onbekend
DroneCategory	Categorie drone	Commercieel / Industriëel / Militair / Zelfgemaakt / Onbekend
DroneWings	Type drone	Fixed-wing / Rotary-wing / Onbekend
DroneModif	Drone gemodificeerd	Ja / Nee / Onbekend
Doelwit en aanslagplan		
TargetCat	Categorie doelwit	Politici / Overheid / Kritieke infrastructuur / Burgers / Rivalen / Anders
PlotLaunched	Aanslagplan uitgevoerd	Ja / Nee
DroneLaunched	Drone gelanceerd	Ja / Nee
PlotSuccFail	Uitkomst aanslag(plan)	Gelukt / Gefaald / Deels gelukt
FailWhy	Reden van falen	Fout van bestuurder / Technische problemen / Verijdeld / Detectie tijdens incident / Neergehaald (Counter-UAS) / Anders
Daderkenmerken		
PerpAttribution	Mate van attributie	Bevestigd / Verdacht / Onbekend
PerpAge	Leeftijd dader	Numeriek / Onbekend
PerpNat	Nationaliteit dader	Tekst / Onbekend
PerpType	Categorie dader	Eenling / Dyade / Terrorist / Georganiseerde misdaad / Statelijke actor
PerpIdeology	Ideologie	Jihadistisch / Rechtsextremistisch / Anders / Geen / Onbekend / Niet van toepassing
PerpAff	Groeps- of staatsaffiliatie	Tekst / Geen / Onbekend
PerpApprehended	Status dader	Gearresteerd / Overleden / Niet gepakt
Motivatie en leerroutes		
DroneWhy	Motivatie voor dronegebruik	Operationeel voordeel / Impact / Toegang (tot hard target) / Onbekend
PracticePerp	Oefening vooraf	Ja / Nee / Onbekend
Learning	Leer- of innovatieroute	Experimentatie / Observatie / Training / Rekrutering / Onbekend

Bibliografie

Boffey, D., & Bryant, M. (2025, oktober 5). 'A collective anxiety attack': The psychology of unexplained drone sightings across Europe. *The Guardian*. https://www.theguardian.com/news/ng-interactive/2025/oct/05/a-collective-anxiety-attack-the-psychology-of-unexplained-drone-sightings-across-europe

Bouhlaoui, A. (2025). *Sky Gates: The Evolution of Improvised Drone Warfare and the Looming Threat of Civilian Terrorism* (SSRN Scholarly Paper No. 5281811). Social Science Research Network. https://doi.org/10.2139/ssrn.5281811

Bunker, R. J., & Sullivan, J. P. (2021a). *Criminal Drone Evolution: Cartel Weaponization of Aerial IEDS*. Xlibris Corporation.

Bunker, R. J., & Sullivan, J. P. (2021b, november 11). Mexican Cartels are Embracing Aerial Drones and They're Spreading. *War on the Rocks*.

Bunker, R. J., Sullivan, J. P., Kuhn, D. A., & Futures, O. (2020). *Use of Weaponized Consumer Drones in Mexican Crime War*. Counter-IED Report.

Dalton, J. (2025, mei 4). Terrorists and criminals misusing 'dark' drones could cause carnage, expert warns. *The Independent*. https://www.independent.co.uk/news/world/americas/dark-drones-attack-crime-ukraine-russia-b2734675.html

Damiani, G., & Jasper, L. (2024). *Looming and Lethal: Assessing the Operational Implications of Drone Use by Mexican Organised Crime Groups*. HCSS.

Dass, R. (2024). Hayat Tahrir al-Sham's Drone Force. *Lawfare*. https://www.lawfaremedia.org/article/hayat-tahrir-al-sham-s-drone-force

Davidse, J. (2024, maart 29). Een lab vol Mexicanen. *Opportuun*, 2. https://magazines.openbaarministerie.nl/opportuun/2024/02/een-lab-vol-mexicanen

Dienst Justitiële Inrichtingen. (2022, mei 16). *Aanpak van smokkelwaar via drones*. Dienst Justitiële Inrichtingen. https://www.dji.nl/actueel/nieuws/2022/05/16/aanpak-van-smokkelwaar-via-drones

Doctor, A. (2025). Rapid Review A: The Logic of Terrorist Use of Unmanned Aerial Systems, Enabling Factors, and Barriers to Exploitation. *Reports, Projects, and Research*. https://digitalcommons.unomaha.edu/ncitereportsresearch/131

Dulligan, J., Freeman, L., Phoenix, A., & Davis, B. (2025). The Rising Threat of Non-State Actor Commercial Drone Use: Emerging Capabilities and Threats. *CTC Sentinel*.

Favia, F., Alsteens, E., Whitehead, K., & Posta, T. (2025). *Meeting the Drone Challenge: The Future of UAVs in Hybrid Warfare - Finabel*. FINABEL. https://finabel.org/meeting-the-drone-challenge-the-future-of-uavs-in-hybrid-warfare/

Haugstvedt, H. (2021). The Right's Time to Fly?: Exploring the Possibility of Right-Wing Extremists' Use of UAVs. *The RUSI Journal*, *166*(1), 22-31. https://doi.org/10.1080/03071847.2021.1906161

Haugstvedt, H. (2024). Still Aiming at the Harder Targets: An Update on Violent Non-State Actors' Use of Armed UAVs. *Perspectives on Terrorism*, *18*(1).

Jager, W. de. (2025, juli 9). Eerste moordaanslag met FPV-drone in Rusland zet politie op scherp. *Dronewatch*. https://www.dronewatch.nl/2025/07/09/eerste-moordaanslag-met-fpv-drone-in-rusland-zet-politie-op-scherp/

Kenyon, J., Binder, J. F., & Baker-Beall, C. (2025). An analysis of terrorist attack perpetrators in England and Wales: Comparing lone actors, lone dyads, and group actors. *Journal of Threat Assessment and Management*, *12*(1), 23-44. https://doi.org/10.1037/tam0000224

Krame, G., & and Davies, A. (2023). Narco drones: Tracing the evolution of cartel aerial tactics in Mexico's low-intensity conflicts. *Small Wars & Insurgencies*, *34*(6), 1095-1129. https://doi.org/10.1080/09592318.2023.2226382

Laumans, W., & Vugts, P. (2026, januari 24). Plegen Amsterdamse criminelen straks liquidaties met drones uit Oekraïne? 'Gebeurde ook bij wapens uit de Balkanoorlogen'. *Het Parool*. https://www.parool.nl/misdaad/plegen-amsterdamse-criminelen-straks-liquidaties-met-drones-uit-oekraine-gebeurde-ook-bij-wapens-uit-de-balkanoorlogen~bc4bb2af/

Lubrano, M. (2023). Navigating Terrorist Innovation: A Proposal for a Conceptual Framework on How Terrorists Innovate. *Terrorism and Political Violence*, *35*(2), 248–263. https://doi.org/10.1080/09546553.2021.1903440

Moghadam, A. (2008). *The globalization of martyrdom: Al Qaeda, Salafi jihad, and the diffusion of suicide attacks*. The Johns Hopkins University Press.

Moore, G. A., & McKenna, R. (2001). *Crossing the chasm: Marketing and selling high-tech products to mainstream customers* (Rev. ed). PerfectBound.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2023). *Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten 2023*. Ministerie van Justitie en Veiligheid. https://www.nctv.nl/onderwerpen/bewaken-en-beveiligen/documenten/circulaires/2023/07/11/circulaire-bewaken-en-beveiligen-2023

Nationaal Coördinator Terrorismebestrijding- en Veiligheid. (2024, juni). *Dreigingsbeeld Terrorisme Nederland Juni 2024*.

O'Connor, F., Malthaner, S., & Lindekilde, L. (2018). Killing in Pairs: Radicalisation Patterns of Violent Dyads. *International Journal of Conflict and Violence (IJCV)*, *12*, a640–a640. https://doi.org/10.4119/ijcv-3099

Parcover, G. (2025, september 9). The Future of Criminal Drone Use in Latin America. *War on the Rocks*. https://warontherocks.com/2025/09/the-future-of-criminal-drone-use-in-latin-america/

Police1. (2018, mei 7). *Criminal gang used drone swarm to obstruct FBI hostage operation*. https://www.police1.com/patrol-issues/articles/criminal-gang-used-drone-swarm-to-obstruct-fbi-hostage-operation-ksbtUD3ltDA4f3S9/

Rai, S. (2025, september 9). Out of the woodwork: Examining the global aspirations of The Base. *ISD*. https://www.isdglobal.org/digital_dispatches/out-of-the-woodwork-examining-the-global-aspirations-of-the-base/

Ramirez, M. H. (2022). Future use of Lethal Autonomous Weapons (LAWs) by criminal Non-State Actors, and its possible effects on governance, national security and democracy. A futures studies analysis for the case of drug cartels in Mexico in 2050. *Futuri*, (18), Article 18.

Rivera, M., Markhoff, B., Tressel, C., & Jones, T. (2025, maart 15). Drone attack warning: Illinois terrorism experts issue risk assessment for potential drone attacks. *ABC7 Chicago*. https://abc7chicago.com/post/drone-attack-warning-illinois-statewide-terrorism-intelligence-center-issues-risk-assessment-potential-attacks/16024421/

Rogers, E. M. (1983). *Diffusion of innovations* (3rd ed). Free press.

Rossiter, A. (2018). Drone usage by militant groups: Exploring variation in adoption. *Defense & Security Analysis*, *34*(2), 113–126. https://doi.org/10.1080/14751798.2018.1478183

Silva, J. R., & Lankford, A. (2024). The globalization of American mass shootings? An assessment of fame-seeking perpetrators and their influence worldwide. *International Journal of Comparative and Applied Criminal Justice*, *48*(2), 119–142. https://doi.org/10.1080/01924036.2022.2162095

Toledano, J. S. (2024, oktober 26). Narco-Drones: The Use of Drones by Drug Cartels. *Grey Dynamics*. https://greydynamics.com/narco-drones-the-use-of-drones-by-drug-cartels/

Van Dongen, T., Veilleux-Lepage, Y., Leidig, E., & Rigault Harkis, H. (2022). *Right-Wing Extremism in the Military* [Research Paper]. International Centre for Counter-Terrorism. https://doi.org/10.19165/2022.1.02

van Gestel, B., & Kouwenberg, R. F. (2021). *Tweede verkennende studie Liquidaties* (No. 3022c; Cahiers 2021-27, p. 53). Wetenschappelijk Onderzoek- en Documentatiecentrum.

van Oosten, F. (2025, november 24). *Antwoord op vragen van het lid Michon-Derkzen over het voorkomen van een terroristische aanslag met een drone op politici in België*.

Veilleux-Lepage, Y., & Archambault, E. (2022). *A Comparative Study of Non-State Violent Drone use in the Middle East*. ICCT. https://doi.org/10.19165/2022.3.01

Auteur
Stijn Willem van ’t Land

Uitgave
juni 2026
Universiteit Leiden
Faculteit Governance & Global Affairs
Turfmarkt 99, 2511 DP Den Haag
In opdracht van het Kenniscentrum
Bewaken en Beveiligen

Meer informatie
bewakenenbeveiligen.universiteitleiden.nl
bewakenenbeveiligen@fgga.leidenuniv.nl

Voor toegang tot de dataset kunt u contact opnemen
met de auteur: s.w.van.t.land@fgga.leidenuniv.nl

Universiteit
Leiden
Institute of Security
and Global Affairs

Kenniscentrum
Bewaken en
Beveiligen