Gespreksnotitie Rathenau Instituut | Rondetafelgesprek Drones en Killer Robots | Tweede Kamer 21 januari 2019, 14.00 – 18.00

Deze gespreksnotitie van het Rathenau Instituut bespreekt diverse uitdagingen omtrent de regulering van de inzet en ontwikkeling van killer robots (deel 1). Daarbij kijken we naar het vraagstuk van betekenisvolle menselijke controle bij de inzet van autonome wapensystemen en naar de vraag hoe de proliferatie van autonome wapensystemen kan worden ingedamd. Daarnaast bespreken we ook het civiele gebruik van drones (deel 2). Het is ook belangrijk voor de commissie Buitenlandse Zaken dat ze voor dit onderwerp aandacht heeft (hoewel de commissie Infrastructuur en Water het voortouw heeft op dit dossier). Het gevaar speelt namelijk dat vanwege het *dual use* karakter van veel roboticatechnologie bepaalde commerciële robotapparaten, zoals civiele drones, relatief eenvoudig kunnen worden getransformeerd tot robotwapens. Vandaar dat we in deze notitie ook kijken naar de manier waarop de veiligheid van civiele drones wordt gereguleerd en hoe het zit met de handhaving daarvan. Bovendien kijken we daarnaast naar de relatie tussen drones en privacy, aangezien dit thema sterk kan raken aan het gevoel van veiligheid van burgers in hun persoonlijke leefomgeving.

1 Regulering van de inzet en ontwikkeling van killer drones

Wereldwijd maken vele politici, wetenschappers en humanitaire organisaties zich ernstige zorgen over de ontwikkeling en inzet van killer robots, waarmee autonome wapensystemen worden aangeduid. Het Europese Parlement heeft bijvoorbeeld op 12 september 2018 een resolutie aangenomen (566 voor en 47 tegen) die oproept tot internationale onderhandelingen over een juridisch instrument om dodelijke autonome wapensystemen te verbieden (2018/2752RSP). Hierbij definieert het Europees Parlement dodelijke autonome wapensystemen als wapensystemen “die zonder betekenisvolle menselijke controle de kritische taken van het kiezen en aanvallen van afzonderlijke doelwitten verrichten”, waarbij wordt toegevoegd dat geautomatiseerde, op afstand bediende systemen geen dodelijke autonome wapens zijn. Op VN-niveau pleiten 28 landen voor een verbod op killer robots.[1] Nederland behoort niet tot die landen. In zijn reactie op het AIV-CAVV-advies “Autonome wapensystemen: De noodzaak van betekenisvolle menselijke controle” uit 2015 geeft het Nederlandse kabinet aan dat het geen voorstander is van een verbod of een moratorium op de ontwikkeling van autonome wapensystemen. Het verwerpt wel de ontwikkeling en inzet van autonome systemen die **niet** onder betekenisvolle menselijke controle staan. De kernvraag daarbij is volgens het kabinet: “Hoe mensen in controle kunnen blijven en de verantwoordelijkheid kunnen blijven dragen voor systemen die in toenemende mate beschikken over een bepaalde mate van autonomie, zelflerend vermogen, of meer in het algemeen kunstmatige intelligentie”.[2] Het heikele punt bij regulering van de inzet van autonome wapensystemen is daarmee wat wordt verstaan onder “betekenisvolle menselijke controle”.

Betekenisvolle menselijke controle bij de inzet van autonome wapensystemen

Bij het adresseren van die vraag dient ten eerste gesteld te worden dat wapensystemen verschillende functies hebben, zoals navigatie, herkenning, transport en doelbestrijding. Betekenisvolle menselijke controle heeft alleen betrekking op de fasen van doelbestrijding. Het

1 https://www.stopkillerrobots.org/wp-content/uploads/2018/11/KRC_CountryViews22Nov2018.pdf
2 https://zoek.officielebekendmakingen.nl/ah-tk-20182019-264.html

doelbestrijdingsproces omvat alle momenten waarop de mens afwegingen maakt over het toepassen van geweld, hetgeen dient te gebeuren binnen de kaders van het humanitair oorlogsrecht.[3] De NAVO omschrijft het doelbestrijdingsproces als volgt: *"Joint targeting is the process of determining the effects necessary to achieve the commander's objectives, identifying the actions necessary to create the desired effects based on means available, selecting and prioritizing targets, and the synchronization of fires with other military capabilities and then assessing their cumulative effectiveness and taking remedial action if necessary."*[4]

Vraag is nu in welke fasen van doelbestrijding welke mate van menselijke controle betekenisvol is. Bij het waarborgen van betekenisvolle menselijke controle kunnen vele factoren een rol spelen.[5] Bij het bepalen van een doelwit en de beslissing om te schieten wordt de mens geïnformeerd door complexe technische systemen die een grote hoeveelheid informatie van verschillende bronnen integreren, filteren, verwerken en interpreteren. In hoeverre is er dan sprake van betekenisvolle controle over dat informatievergaringsproces? Deze vraag is al relevant bij de huidige op afstand bestuurbare bewapende militaire drones.[6] Daarnaast speelt de vraag op welk moment de mens in betekenisvolle controle dient te zijn. Als bijvoorbeeld de mens het doelwit heeft bepaald, mag een wapensysteem dit doel dan autonoom uitschakelen, of is bij die aanval dan ook menselijke controle noodzakelijk? Roff & Moyes stellen: *"A human simply pressing a 'fire' button in response to indications from a computer, without cognitive clarity or awareness, is not sufficient to be considered 'human control' in a substantive sense."*[7] Bij de inzet van AI speelt de vraag in hoeverre er sprake is van zogenaamde "*explainable AI*": AI waarvan de acties voorspelbaar en uitlegbaar zijn.

Kortom, voor de regulering van zowel de inzet van autonome wapensystemen die onder betekenisvolle menselijke controle staan (Nederland) als voor een verbod op de inzet van autonome wapensystemen zonder betekenisvolle menselijke controle (Europees Parlement), is het belangrijk om tot overeenstemming te komen over:

- Wat betekent "betekenisvolle menselijke controle" in de verschillende fasen van doelbestrijding?
- Hoe kunnen autonome wapensystemen ontworpen worden zodat "betekenisvolle menselijke controle" mogelijk is (*ethics by design*)?

Beantwoording van deze kwesties is urgent omdat de ontwikkeling van autonome wapensystemen in een zeer ver stadium is gevorderd.[8] Een interessante aanzet om over deze vragen na te denken wordt gegeven door Ekelhof (2015).[9] Zij stelt dat de volgende vier factoren houvast kunnen bieden in het bepalen of menselijke controle betekenisvol is: 1) controle door middel van programmering; 2) geografische controle; 3) temporele controle; en 4) de mate van voorspelbaarheid. Met betrekking tot het eerste punt bijvoorbeeld kan de mens de specificatie van de parameters voor doelselectie bepalen, zodat bij de uitvoering het systeem voorspelbaar is in het kiezen van het doel. Dus ondanks de autonome functies opereert het systeem dan

---

3 https://www.clingendael.org/sites/default/files/pdfs/KNV_ARMEX_Artikel_P24-25.pdf

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/628215/-20160505-nato_targeting_ajp_3_9.pdf

5 Zie bijvoorbeeld M. Ekelhof (2015) Autonome wapens: een verkenning van het concept Meaningful Human Control. Militaire Spectator 184 (5) 232-245.

6 Royakkers, L.M.M en R. van Est (2010) The cubicle warrior: the marionette of digitalized warfare. Ethics and Information Technology 12(3), 289-296.

7 Roff, H.M. & R. Moyes (2016). Meaningful Human Control, Artificial Intelligence and autonomous Weapons. Briefing paper prepared for the Informal Meeting of Experts on Lethal Autonomous Weapons Systems, UN Convention on Certain Conventional Weapons, April 2016.

8 Royakkers, L. & R. van Est (2016) Just ordinary robots: Automation from love to war. Boca Raton: CRC Press.

9 Ekelhof, M. (2015). Autonome wapens: een verkenning van het concept Meaningful Human Control. Militaire Spectator, 184(5), 232-245.

feitelijk onder menselijke controle met betrekking tot doelselectie. Van belang hierbij is dat deze systemen niet zelflerend zijn, omdat dan die controle wegvalt.

Indammen van de proliferatie van autonome wapensystemen

Wereldwijd wordt veel geld geïnvesteerd in de ontwikkeling van autonome wapensystemen, zoals in de Verenigde Staten, China, Rusland, Groot-Brittannië, Canada, Israël, Singapore en Zuid-Korea. Dit signaleert het begin van een internationale wedloop op autonome wapens, waardoor proliferatie naar andere landen, inclusief schurkenstaten en terroristische groeperingen, op de loer ligt. Duizenden AI- en robotica-experts vrezen dat "*by removing the risk, attributability, and difficulty of taking human lives, lethal autonomous weapons could become powerful instruments of violence and oppression, especially when linked to surveillance and data systems*".[10]

Proliferatie is vrijwel onontkoombaar omdat, in tegenstelling tot andere wapensystemen, het onderzoek en de ontwikkeling van autonome wapensystemen vrij transparant en toegankelijk zijn. Veel roboticatechnologie kent *dual use* en heeft toepassingen voor zowel de militaire als civiele markt. Een gevaar is dat bepaalde commerciële robotapparaten, zoals autonome voertuigen en civiele drones, relatief eenvoudig kunnen worden getransformeerd tot robotwapens. De kans is dan ook groot dat instabiele landen en terroristische organisaties bewapende (autonome) militaire robots gaan inzetten.

Het Nederlandse kabinet heeft in 2015 aangegeven geen voorstander te zijn van een moratorium op de ontwikkeling van autonome wapensystemen. Ten behoeve van het aanstaande actieplan inzake de Nederlandse inzet bij de internationale beheersing van drones en killer robots - dat in april 2019 uit zal komen - dient Nederland desalniettemin de vraag te adresseren hoe een mondiale wapenwedloop, en in het verlengde daarvan de proliferatie van autonome wapens, tegengegaan kan worden. Juist het *dual use* karakter van dronetechnologie maakt dit een zeer lastige vraag. De vraag rijst namelijk "een verbod op wat?".[11] Gegeven het immense destabiliserende effect van de mogelijke proliferatie van autonome wapens dient het (preventief) indammen daarvan een belangrijk aandachtspunt te zijn bij de ontwikkeling van robotica en AI, zelfs als nuttige civiele ontwikkelingen daarvan hinder kunnen ondervinden.

2 Regulering van het gebruik van civiele drones

In juni 2018 heeft het Europees Parlement ingestemd met de voorgestelde drone-regelgeving (zie kader 1) opgesteld door het European Aviation Safety Agency (EASA).[12] Deze regelgeving gaat medio 2019 in en zal op termijn de regelgeving modelvliegen en de regeling op afstand bestuurbare luchtvaartuigen vervangen. In de regelgeving wordt ingegaan op veiligheid, privacy, aansprakelijkheid en bewijslevering. Hoewel de nieuwe regelgeving een stuk helderheid brengt, blijft een aantal urgente vraagstukken met betrekking tot veiligheid en privacy onderbelicht.[13]

Veiligheid: lastige opsporing en handhaving

Volgens de nieuwe EU-regelgeving dienen drones uitgerust te zijn met *geo-awareness* zodat bestuurders een waarschuwing krijgen wanneer ze in de buurt van vliegvelden komen of boven

10 https://futureoflife.org/lethal-autonomous-weapons-pledge/.
11 https://zoek.officielebekendmakingen.nl/ah-tk-20182019-264.html
12 https://www.easa.europa.eu/sites/default/files/dfu/Opinion%20No%2001-2018.pdf.
13 We merken op dat de inzet van civiele drones, naast veiligheid en privacy, ook kunnen raken aan publieke waarden zoals autonomie, controle over technologie, rechtvaardigheid, menselijke waardigheid (zie Kool, L., J. Timmer, L. Royakkers & R. van Est (2017) Opwaarderen - Borgen van publieke waarden in de digitale samenleving. Den Haag: Rathenau Instituut.)

de maximaal toegestane hoogte vliegen. Zij krijgen dan een waarschuwing en zijn zelf verantwoordelijk voor het vermijden van *no-fly zones*. In veel gevallen ligt enkel waarschuwen via *geo-awareness* inderdaad voor de hand. Men kiest in dat geval voor zelfregulering via *nudging*; het geven van een duwtje in de juiste richting, zonder hierbij vrijheden in te perken of verplichtingen op te leggen. In sommige gevallen lijkt echter techno-regulering via een striktere vorm van *geofencing* vanuit het perspectief van veiligheid de voorkeur te hebben. Het virtuele hek geeft daarbij instructies aan de autopilot van de drone en kan deze zelfs dwingen om te landen. De ervaring leert dat het gevaar voor bijna-botsingen tussen vliegtuigen en drones groot is en toeneemt. Eind 2018 lag de Londense luchthaven Gatwick een etmaal stil vanwege twee waargenomen drones. Het feit dat meer dan twintig politie- en legereenheden werden ingezet om de drones te pakken, geeft aan hoe lastig opsporing en handhaving op dit moment is. Het is daarom de moeite waard de kansen en risico's voor striktere vormen van *geofencing* verder te onderzoeken. Dit is tevens van belang vanuit het hierboven onder paragraaf 1 reeds genoemde gevaar dat civiele drones relatief eenvoudig kunnen worden getransformeerd tot robotwapens en het van belang kan zijn in hoe we ons hiertegen kunnen gaan beschermen.

Daarnaast is het onduidelijk wat de betekenis van regelgeving voor reeds verkochte drones of zelfgebouwde drones boven de 250 gram is en welke kenniseisen gevraagd worden in de onlinetest. Tevens is onduidelijk hoe de notie "uit de buurt van mensen" geïnterpreteerd dient te worden.

Kader 1 Nieuwe EU droneregelgeving in het kort

In de nieuwe regelgeving worden vijf klassen drones onderscheiden: C0 tot en met C4. Met uitzondering van drones die vallen onder klasse C0 (tot 250 gram), is er een verplichting om drones identificeerbaar te maken door een chip met een unieke registratiecode. Handhavers kunnen dan op afstand zien welke drones op dat moment, op welke plek vliegen. Daarnaast moeten deze drones zijn uitgerust met *geo-awareness*, waardoor de dronebestuurder gewaarschuwd wordt als hij/zij in de buurt van vliegvelden en andere *no-fly zones* komt. Bovendien moet de dronebestuurder met een onlinetest aantonen voldoende dat hij/zij theoretische kennis heeft en dat hij/zij 14 jaar of ouder is (klasse C1) of 16 jaar en ouder (klasse C2 t/mC4). Voor de C2-(900 gram tot 4 kilo), C3-(4 tot 25 kg) en C4-(25 kilo) klassen gelden oplopende eisen aan de dronebestuurder en de wijze waarop de vlucht moet worden uitgevoerd. Voor alle klassen geldt een maximale vlieghoogte van 120 meter, en geen beperking ten aanzien van de maximale afstand tot de bestuurder, zolang de drone maar in zicht blijft. Daarnaast geldt voor de klassen C0 en C1 (250 tot 900 gram) dat er boven andermans grondgebied gevlogen mag worden (maar niet over groepen mensen). Voor de klasse C2 geldt dat ze wel over groepen mensen mogen vliegen met een minimale vlieghoogte van vijf meter (daarbij is wel een extra theoretische test vereist), en voor de klassen C3 en C4 dat ze uit de buurt van mensen moeten blijven en buiten de bebouwde kom. Voor alle klassen geldt dat er met het oog op privacy geen foto's of filmopnamen gemaakt mogen worden van mensen tenzij zij daar expliciet toestemming voor hebben gegeven.

Weinig aandacht voor privacy

Binnen de nieuwe regelgeving is weinig aandacht voor bescherming van privacy. Er is opgenomen dat er geen foto's, filmopnamen of geluidsopnamen van mensen mogen worden gemaakt, zonder hun toestemming. Deze zinsnede adresseert de privacykwesties die rondom civiele drones kunnen spelen niet adequaat. Door snelle technologische ontwikkelingen op het gebied van infraroodsensoren, geluidsensoren en camera's maar ook de mogelijkheden van drones om iets op te pakken en te laten vallen alsmede miniaturisering kunnen mensen drones in toenemende mate als bedreigend ervaren. Daarbij zijn drones ook niet altijd zichtbaar en is het lastig inschatten wat het doel van een drone is en wat deze precies doet; alleen vliegen, opnames maken of zelfs een explosief bij zich dragen? Burgers kunnen zo het gevoel krijgen dat ze constant geobserveerd worden en hun veiligheid in het geding is. In de nieuwe regelgeving mogen drones van de klasse C0 over andermans grondgebied vliegen en juist deze drones worden vaak gebruikt als op afstand bestuurbare vliegende camera's. Een wereldbeeld met autonome miniatuur drones waarvan onbekend is met welk doel ze rondvliegen wordt steeds reëler. Moeten burgers zich af gaan vragen of het een drone met commerciële-, surveillance- of militaire doeleinden is, die rond vliegt?

De vraag hoe we een wereld voorkomen waarin we elkaar continu bespieden of ons continu bespied voelen, is eveneens zeer relevant. Dit roept kwesties op omtrent horizontale en verticale privacy en autonomie. Verticale privacy betreft hoe overheid en industrie omgaan met de privacy van burgers, en horizontale privacy gaat over hoe burgers met elkaars privacy omgaan. Autonomie is in het geding als het gevoel constant te worden begluurd leidt tot zelfcensuur of

conformistisch gedrag. De nieuwe regelgeving beschermt de burger onvoldoende tegen opzettelijke of onopzettelijke dronesurveillance.

Aangaande privacy komen we tot de volgende punten die verdere aandacht vergen:

- De huidige regelgeving vereist voor de drones klasse C0 geen toestemming om boven andermans grondgebied te vliegen. Voor de andere klassen is toestemming slechts vereist als ze lager dan 20 meter vliegen. De wetgever vertrouwt daarmee teveel op de sociale etiquette en onderschat het risico dat burgers elkaar bespieden of bedreigen;
- Het is niet helder wat onder toestemming van mensen voor het maken van foto's en filmopnamen wordt verstaan en of het geven van toestemming ook geldt voor personen die onherkenbaar in beeld komen;
- Het is niet duidelijk hoe de bescherming van privacy van burgers kan worden gehandhaafd;
- Het is onduidelijk in hoeverre (lokale) overheden binnen de afzonderlijke lidstaten zeggenschap hebben over het instellen van "no-fly zones";
- Verdere miniaturisering van drones zal leiden tot nieuwe toepassingen die ook de kans verhogen op inbreuk op het recht van privacy.

Het zou goed zijn om bij de nationale implementatie en uitvoering van de regelgeving rekening te houden met bovenstaande vijf punten.[14]

Tot slot houdt de nieuwe regelgeving geen rekening met de mogelijkheid tot autonome vluchten met drones, die voor veel toepassingen, zoals bezorging per drone, noodzakelijk zijn. De logistiek en *supply chain* sector willen in de toekomst autonome drones inzetten, maar zijn nog terughoudend om hierin te investeren vanwege gebrek aan wet- en regelgeving. Om de mogelijkheden van autonome drones optimaal te benutten is het van belang om duidelijkheid te scheppen op het gebied van wet- en regelgeving.[15] Zoals de wetgeving nu is, zijn vluchten met autonome drones niet toegestaan. Daarnaast is het belangrijk om bij nieuwe toepassingen, zoals de bezorgdrone, na te gaan welke maatschappelijke kansen en dilemma's gaan spelen. Ook hier speelt bijvoorbeeld de *dual use* kwestie: slimme voertuigen als bezorgdrones, kunnen tevens als moordwapen ingezet kunnen worden.

14 Het rapport Drones en privacy: Handleiding voor een gebruik van drones dat voldoet aan de waarborgen voor bescherming van de privacy uit 2015 kan daarbij voor inspiratie zorgen: Zie https://www.rijksoverheid.nl/onderwerpen/drone/documenten/rapporten/2015/12/02/tk-drones-en-privacy.

15 http://files.smart.pr/57/a6d8301fa011e7afd66dd397d97932/Hays-rapport-Baan-van-de-Toekomst-sector-logistiek---supply-chain.pdf.