Rathenau Instituut

Maatregelen voor cybervrede

Betere regulering van technologisch nieuwe wapensystemen

Bericht aan het Parlement

Op 3 oktober a.s. is het AO Technologisch nieuwe wapensystemen van de vaste Kamercommissie Buitenlandse Zaken. Deze wapensystemen zijn in toenemende mate gebaseerd op *dual use* technologie, zoals drones en hacksoftware. Technologie die zowel voor civiele als militaire toepassingen gebruikt kan worden. Het is van belang om de *ontwikkeling* van *dual use* technologie verstandig te sturen. Daarnaast creëert de *inzet* van nieuwe wapensystemen nieuwe uitdagingen, zoals een cyberwapenwedloop. Ook deze uitdagingen vragen om verstandige regulering. Dit bericht aan het Parlement bevat beleidsopties om tot een verstandige regulering van zowel de ontwikkeling als de inzet van technologisch nieuwe wapensystemen te komen.

Inleiding

De afgelopen jaren is het onderscheid tussen civiel of militair gebruik van technologie vervaagd. Dit komt met name door de opkomst van digitale technologie: robotica en AI kennen naast civiele ook militaire toepassingen – denk aan een geautomatiseerde gevechtsdrone. Civiel universitair onderzoek kan een rol spelen in een militaire wapenwedloop, of de individuele onderzoeker dit nu wil of niet. Bovendien heeft de digitalisering van de samenleving allerlei nieuwe veiligheidsrisico's gecreëerd. Banken, havens en ziekenhuizen kunnen allemaal door cyberaanvallen getroffen worden, en dat gebeurt ook. Dit maakt het extra belangrijk dat digitale technologie op een verstandige manier wordt onderzocht, ontwikkeld en ingezet.

Beheersing van de ontwikkeling van *dual use* technologie is bij uitstek een internationaal vraagstuk. Landen als China, de Verenigde Staten, Frankrijk en Duitsland concurreren met elkaar om een voorsprong op te bouwen in de ontwikkeling van veelbelovende technologie – denk aan AI –, en daarmee zowel economisch als militair invloed uit te oefenen. In Europees verband wordt steeds meer geld voor onderzoek naar technologie beschikbaar gesteld die *dual use* toepassingen kennen. Er zijn allerlei organisaties en bedrijven in tal van landen actief die dual use technologie ontwikkelen. Dit betekent dat de beheersing van *dual use* technologie deels vraagt om internationale acties, en deels om een duidelijke opstelling van de Nederlandse overheid in Europese en mondiale gremia.

Ook de inzet van technologisch nieuwe wapensystemen verandert het internationale speelveld. Er vindt ten aanzien van cybermiddelen een wapenwedloop plaats. Er worden autonome wapensystemen ontwikkeld die grote ethische vragen oproepen, bijvoorbeeld de vraag wie verantwoordelijk is voor wat deze wapensystemen doen. De inzet van allerlei soorten drones vraagt om het verhelderen van conceptuele, juridische en beleidsmatige kaders. Dit is belangrijk in het kader van het bepalen van de respons op een eventuele drone aanval met als doel om zo snel mogelijk de schade te beperken.

Dit bericht stelt een aantal beleidsopties voor, die deels van toepassing zijn op **onderzoek en ontwikkeling** van *dual use* technologie (paragraaf 1), en deels betrekking hebben op de **inzet** van technologisch nieuwe wapensystemen (paragraaf 2). Ook roepen we op tot een geïnformeerd maatschappelijke **dialoog** (paragraaf 3).

1. Reguleer onderzoek en ontwikkeling van *dual use* technologie

Het Rathenau Instituut bepleit in de studie *Kennis in het vizier* (2019) voor behoedzaamheid in de ontwikkeling van technologieën die potentieel militaire toepassingen hebben. Deze behoedzaamheid moet georganiseerd worden. Zodra technologieën eenmaal ontwikkeld zijn en worden toegepast, is het immers lastiger ze beheersen. Dat blijkt wel uit de discussie over de EU *dual use* verordening.

De EU *dual use* verordening is één van de belangrijkste reguleringsinstrumenten ten aanzien van *dual use* technologie. Als een technologie op de lijst behorend bij deze verordening staat, moeten bedrijven een speciale vergunning hebben om de technologie te verhandelen. Het blijkt ten aanzien van sommige *dual use* technologieën, zoals digitale surveillancetechnologie, moeilijk om met voldoende lidstaten dezelfde positie in te nemen en de lijst uit te breiden. Als de technologie eenmaal is ontwikkeld en wordt toegepast, blijkt controle daarop lastig te zijn.

Dit betekent niet dat de huidige EU *dual use* verordening zijn nut heeft verloren. Maar het betekent wel dat gezocht moet worden naar proactieve aanvullende acties. We stellen de volgende voor:

1.1 Investeer in onderzoek naar de impact van *dual use* technologie

Inzicht krijgen in de risico's van *dual use* technologie begint bij onderzoek. Niet alleen het ontwikkelen van *dual use* technologie is belangrijk, maar ook het onderzoeken van de mogelijke impact van *dual use* technologie. Onderdeel hiervan is het verhelderen van definities: wanneer is een drone een militair wapen, en wanneer is het een civiele toepassing? Wanneer spreken we van een cyberwapen, of van een cyberoorlog? En in hoeverre hebben we de technologie nog voldoende onder controle? Op het gebied van cyberaanvallen heeft het Rathenau in de studie *Cyberspace zonder Conflict* deze begripsvragen geïdentificeerd. Meer onderzoek is nodig om de juridische, beleidsmatige en maatschappelijke gevolgen van de ontwikkeling van *dual use* technologie te doordenken.

Het kabinet heeft aangegeven de mogelijkheden te bezien om periodiek de implicaties van nieuwe technologische ontwikkelingen voor de nationale veiligheid in kaart te brengen. Het zal significante onderzoekscapaciteit vergen om de impact van *dual use* technologie goed in kaart te brengen, en steeds de juiste conceptuele, technische, bestuurlijke en ethische vragen te stellen. Gezien de genoemde ontwikkelingen moet het kabinet hier niet mee wachten.

1.2 Doordenk de rol van veiligheid in het kennisecosysteem

De grens tussen civiele en militaire technologie vervaagt steeds meer. Dit betekent dat in het civiele onderzoek van universiteiten, hogescholen en publieke kennisorganisaties steeds vaker veiligheidsafwegingen gemaakt moeten worden. Kunnen de resultaten gebruikt worden voor gevaarlijke doeleinden? Deze vraag moet niet bij individuele onderzoekers worden neergelegd. Een gecoördineerde aanpak is nodig, waarbij alle relevante civiele kennisinstellingen hetzelfde beleid volgen. Het is onwenselijk dat bepaald onderzoek toegestaan wordt aan de TU Delft, maar niet aan de TU Eindhoven, of andersom. Het is aan de Rijksoverheid de beleidskaders te scheppen, opdat de kennisinstellingen deze verder kunnen invullen.

Deze beleidskaders gaan niet alleen over de inhoud van het onderzoek, maar ook over zaken als de omgang met *open science* in het licht van geopolitieke ontwikkelingen, het werven van buitenlandse werknemers, de toegang van buitenlandse partners tot de fysieke en digitale infrastructuur van kennisinstellingen, de bronnen van financiering en de internationale samenwerking.

Het zou verstandig kunnen zijn om binnen de instellingen, analoog aan ethische commissies die toezien op ethische aspecten van wetenschappelijk onderzoek, veiligheidscommissies in te richten. Zo hebben verschillende Duitse universiteiten commissies voor *ethical conduct of security-relevant research* ingesteld. Ook moet in alle relevante financieringsprogramma's de eis opgenomen worden dat onderzoekers zelf vanaf het begin belangrijke vragen stellen over veiligheidsaspecten. Hier zijn de financieringsinstellingen zoals het NWO en de DG for Research and Innovation van de Europese Commissie aan zet. Ten slotte is het verstandig dat veiligheidsorganisaties, zoals de NCTV en het ministerie van Defensie, waar nodig betrokken worden en capaciteit beschikbaar stellen.

2. Beheers de inzet van technologisch nieuwe wapensystemen

Er worden momenteel tal van technologisch nieuwe wapensystemen in de praktijk ingezet. Het Rathenau Instituut richt zich in dit Bericht aan het Parlement op drie soorten digitale wapens: cyberwapens, autonome wapensystemen en drones.

2.1 Cyberwapens: zet in op de-escalatie

In onze studie *cyberspace zonder conflict* wijst het Rathenau Instituut op het belang van de-escalerende maatregelen die op de lange termijn de digitale samenleving beter beveiligen. Daarvoor hebben we vijf verschillende acties voorgesteld die een slimme samenwerking tussen de relevante actoren ondersteunen. Ter illustratie contrasteren we deze met de *Nobody but Us* (NOBUS) strategie, die vaak gehanteerd wordt door de Amerikaanse inlichtingendiensten en die de internationale samenwerking juist bemoeilijkt.

NOBUS	**Slim samenwerken**
We zijn leidend	Internationale samenwerking met bondgenoten
Internationale afspraken verkleinen onze voorsprong	Heldere internationale afspraken
Ons beheer is goed, we delen geen kwetsbaarheden	Verantwoord beheer cyberarsenaal, we delen kwetsbaarheden

Technologiebedrijven dwingen hun beveiliging aan te passen	Onafhankelijkheid van technologiebedrijven waarborgen, bijvoorbeeld door encryptie te stimuleren
Cyberveiligheid is iets voor de veiligheidsdiensten	Publiek debat over cyberveiligheid

We lichten er twee acties uit die van bijzonder belang zijn voor de opstelling van Nederland op internationaal niveau: het maken van heldere internationale afspraken en een verantwoord beheer van het cyberarsenaal.

2.1.1 Heldere internationale afspraken

Nederland heeft op het gebied van internationale afspraken al veel goede stappen gezet, van het opzetten van een netwerk van cyberdiplomaten tot het aanschuiven bij de laatste editie van de UN Group of Governmental Experts on the Development in the Field of Information and Telecommunications in the Context of International Security (UNGGE). Bovendien is er op EU-niveau een sanctieregime ingesteld, waarbij overheden cyberaanvallers een reisverbod kunnen opleggen en financiële middelen kunnen bevriezen.

Maar meer is nodig. Nederland kan zich binnen de UN GGE verder inzetten voor wereldwijde, bindende afspraken die zijn toegespitst op cyberaanvallen. Daarnaast is het belangrijk dat Nederland ook in kleinere verbanden, zoals de G7, duidelijk maakt welke afspraken nodig zijn. Op het mondiale overleg kan namelijk niet gerekend worden – te meer daar de normontwikkeling niet meer alleen via de UN GGE verloopt, maar ook via de Open Ended Working Group, het door Rusland geleide parallelle gremium. Beide gremia kunnen verschillende en tegenstrijdige uitkomsten opleveren.

Ook moet voorkomen worden dat de Nederlandse offensieve inzet van cybermiddelen een risico vormt voor de diplomatieke inzet. De onthullingen over de Stuxnet-operatie tonen aan dat cyberaanvallen serieuze gevolgen hebben voor de internationale verhoudingen.

2.1.2 Verantwoord beheer cyberarsenaal

Om de wapenproliferatie tegen te gaan is het van belang om samen te werken met bondgenoten en gezamenlijk kwetsbaarheden te melden aan de bouwers van digitale toepassingen. Ook een helder nationaal afwegingskader voor het melden van kwetsbaarheden, zoals voorgesteld door Kamerlid Verhoeven, is hier op zijn plaats. Bovendien is het van belang dat veiligheidsdiensten hacksoftware doordacht gebruiken, en zorgen dat deze technologie niet in verkeerde handen valt. Eenmaal gebruikt, kunnen cyberwapens immers gekopieerd worden en tegen je gebruikt worden. Denk aan het EternalBlue *exploit*, ontwikkeld door de Amerikaanse National Security Agency (NSA), dat uiteindelijk ook gebruikt is door hackergroepen bij de WannaCry en

NotPetya aanvallen. Ten slotte is het belangrijk onderzoek en ontwikkeling van technologie met *dual use* toepassingen goed te sturen, zoals hierboven al besproken is.

2.2 Autonome wapensystemen: maak duidelijk wat betekenisvolle menselijke controle inhoudt

Autonome wapens zijn wapens die, door middel van kunstmatige intelligentie, op verschillende niveaus beslissingen nemen over het aanvallen van bepaalde doelwitten. Dat betekent dat de menselijke controle over de inzet van levensgevaarlijke wapens onder druk staat. Voor dit gevaar is al door vele partijen gewaarschuwd, waaronder VN-secretaris Antonio Guterres. Nederland is geen voorstander van een moratorium op autonome wapens, en pleit in plaats daarvoor voor het centraal stellen van betekenisvolle menselijke controle zodat het huidige internationaal recht volstaat en geen aanvullende regelgeving nodig is.

Toch is tot op heden onduidelijk wat we precies onder deze controle moeten verstaan, zoals we al lieten zien in onze bijdrage aan het rondetafelgesprek Drones en killer robots. Denk hier aan een mens, die bij het bepalen van de inzet van een autonoom wapen geïnformeerd wordt door complexe technische systemen. Deze systemen integreren, filteren, verwerken en interpreteren een grote hoeveelheid informatie van verschillende bronnen. In hoeverre is er dan sprake van betekenisvolle menselijke controle over dat informatievergaringsproces? Het is van belang dat hier helderheid over komt. Pas dan kan de keuze voor een bepaalde juridische regulering van autonome wapens goed bediscussieerd worden.

2.3 Drones: zorg voor een heldere taakverdeling

Dronetechnologie is *dual use* technologie *pur sang.* Drones worden voor onschuldige civiele toepassingen gebruikt, zoals het opnemen van beelden in de natuur of het vervoeren van goederen. Maar ze kunnen ook grote schade aanrichten. Je kan immers ook een explosief vastmaken aan een drone – om niet te spreken over de dronevliegtuigen die door militairen ingezet worden.

Het is daarom belangrijk om goed te onderscheiden welke partij wanneer verantwoordelijk is voor de respons op een drone. Als een kleine drone illegaal door de stad vliegt, moet de brandweer dan uitrukken, de politie, of wellicht het leger? Hier is helderheid nodig. Dit zou kunnen in de Omgevingsvisie en het Omgevingsplan, dat gemeentes in het kader van de Omgevingswet moeten opstellen. In de Omgevingsvisie moeten gemeentes hun visie op het waarborgen van de externe veiligheid geven. In het Omgevingsplan moet zij algemene instructieregels voor de externe veiligheid vaststellen. Daarbij is het wederom goed om zoveel mogelijk te de-escaleren. Als de brandweer een probleem aankan, moet de brandweer, en niet het leger, het probleem oplossen.

3. Nieuwe wapens vragen om publieke dialoog

De opkomst van *dual use* technologie en nieuwe digitale wapensystemen stellen de politiek voor fundamentele keuzes. Sluiten we ons aan bij de offensieve ambities van landen als de VS, of kiezen we voor diplomatie en de-escalatie? Ondersteunen we de opkomst of de ontmanteling van autonome wapens? Onderzoeken we de uitdagingen van dronetechnologie, of trekken we daar liever geen geld voor uit?

Die keuzes kunnen niet uitsluitend in geheime overleggen en expertmeetings gemaakt worden. Dit gaat burgers aan die in het kruisvuur staan. Hun ziekenhuizen en havens worden met virussen onveilig bestookt en drones maken hun vliegvelden onveilig. Burgers worden misleid door desinformatie van vijandige statelijke actoren. Bovendien zijn het voor een groot deel burgers die met password managers en verstandig wifigebruik Nederland veilig moeten houden. Hoe groter de impact van technologische nieuwe wapensystemen en internationale cyberconflicten op de samenleving, des te groter het belang om een relevant publieke dialoog hierover mogelijk te maken.

Bronnen

Diercks, G., J. Deuten en P. Diederen (2019). Kennis in het vizier – De gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur. Den Haag: Rathenau Instituut.

Hamer, J., R. van Est, L. Royakkers, met medewerking van N. Alberts (2019). Cyberspace zonder conflict – Op zoek naar de-escalatie van het internationale informatieconflict. Den Haag: Rathenau Instituut.

Rathenau Instituut (2018). Uitdagingen voor regulering van drones en killer robots. Gespreksnotitie.

Geert Munnichs, Matthijs Kouw & Linda Kool (2017). Een nooit gelopen race – Over cyberdreigingen en versterking van weerbaarheid. Den Haag: Rathenau Instituut.

