Ruimtewapens: fictie of realiteit?

Deel 3: Niet-kinetische ASAT

Henk H.F. Smid

Op 18 juni 2018 kondigde de Amerikaanse president Trump aan: 'We are going to have the Space Force'. Deze aankondiging zorgde voor extra aandacht in de media op het gebied van ruimtewapens. In deel 1 en 2 van deze serie werd een overzicht gegeven van de kinetische ASAT programma's van Amerika, Rusland en China. In dit deel wordt een overzicht gegeven van de huidige stand van zaken op het gebied van niet-kinetische ASAT.

Een toenemend aantal landen en commerciële partijen maken gebruik van de ruimte voor zaken als waarneming (meteorologie, inlichtingen, verkenning), communicatie en navigatie. Deze zaken zijn al lang niet meer voorbehouden aan de grote mogendheden. Het toenemende gebruik van en het vertrouwen op in de ruimte gestationeerde middelen voor nationale veiligheidsdoeleinden leidt er toe dat steeds meer landen zich toeleggen op de verdediging van die middelen. Landen die de noodzaak daarvan inzien ontwikkelen daarom *Counterspace* activiteiten en technieken. Defensieve Counterspace helpt je je eigen middelen te beschermen terwijl offensieve Counterspace moet voorkomen dat je tegenstander zijn ruimtemiddelen kan aanwenden. Tot de offensieve Counterspace behoren bijvoorbeeld antisatelliet wapens (ASAT). Deze groep van wapens kan worden gebruikt om de ruimtecapaciteiten van de tegenstander te verminderen door het toepassen van verstoring, misleiding, ontzegging, degradatie of zelfs vernietiging van de drie systeemelementen van ruimtemiddelen: de satelliet, het grondstation en/of de communicatie daartussen. ASAT wapens kunnen worden verdeeld in vijf soorten. De drie hier laatst genoemde soorten, gezamenlijk Niet-Kinetische ASAT genoemd, worden in dit deel behandeld.

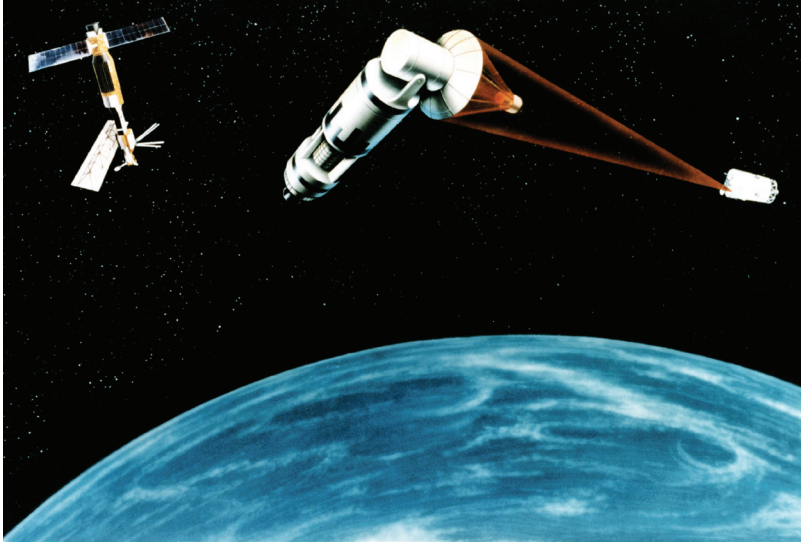
- **Co-orbital** (CO). Kinetische wapens die door raketten in de ruimte worden gebracht en daar afwachten totdat zij naar het doel worden geleid (zie deel 1 in Ruimtevaart 2018|4);
- **Direct Ascent** (DA). Het gebruik van door raketten in de ruimte gebrachte onderscheppers die rechtstreeks het doel met kinetische energie (botsing en/of ontploffing) vernietigen (zie deel 2 in Ruimtevaart 2019|1);
- **Directed Energy** (DE). Wapens die geconcentreerde energie (laser, deeltjes- of microgolfbundels) gebruiken om de werking van het doel te verminderen of te doen stoppen;
- **Electronic Warfare** (EW). Wapens die gebruik maken van radiofrequentie-energie om bijvoorbeeld verbindingen tussen systeemelementen te verstoren;
- **Cyber Warfare** (CW). Wapens die software- en netwerktechnieken gebruiken om computer netwerken te compromitteren of te verstoren, of zelfs computersystemen te vernietigen.

Niet-Kinetische (NK)-ASAT

Onder een niet-kinetisch Anti Satelliet (NK-ASAT) wapen wordt hier verstaan een wapen dat géén gebruik maakt van een grond- lucht- of zee gelanceerde raket om met een meegevoerde onderschepper satellieten kinetisch te vernietigen door een botsing of een nabije ontploffing.

De nucleaire optie

De Amerikanen en Russen hebben sinds het einde van de vijftiger jaren ASATs ontwikkeld. De eerste generatie ASATs waren niet-nucleair- of nucleair geladen ballistische raketten. De niet-nucleair geladen ballistische raket moest de sa-

Links: Starfish Prime detonatie [Los Alamos National Laboratory]. Rechts: Artistieke afbeelding van een Space Laser Satellite Defense System. [USAF]

telliet direct raken of moest nabije satellieten vernietigen door rondvliegende bomscherven. In het geval van nucleair geladen raketten moest de satelliet worden vernietigd door de effecten van de nucleaire detonatie.

Amerika ontwikkelde en testte in het begin exo-atmosferische nucleaire (1 kT) ASATs. Op 9 juli 1962 lanceerden de Amerikanen (oefening Starfish Prime) vanaf Johnson Island op een Titan raket een 1,4 MT nucleair wapen dat op 400 km hoogte tot ontploffing werd gebracht. De lichtflits was tot op Hawaii te zien. Verwacht werd dat een doel zou worden vernietigd door de thermische schokgolf, röntgenstraling of andere stralings- of elektromagnetische effecten. Na de nucleaire detonatie volgden energetische bèta deeltjes het aards magnetisch veld en verlichtten de hemel. Elektronen vormden een stralingsgordel rond de aarde. Er bestond toen nog geen duidelijk beeld van wat er precies zou kunnen gebeuren v.w.b. de samenstelling en sterkte van deze stralingsgordel. Men wist ook niet wat voor negatieve effecten voor andere (ook de eigen) satellieten deze stralingsgordel zou kunnen hebben. Al snel bleek dat drie satellieten in lage aardomloop onklaar waren geraakt. In de maanden daarna raakten nog eens minstens zes satellieten door de stralingsgordel onklaar doordat de zonnepanelen en/of elektronische componenten door de straling werden aangetast. De eerste commerciële satelliet Telstar en de Engelse satelliet Ariel-1 werden eveneens beschadigd. Ook de Sovjet Unie testte met vergelijkbare resultaten nucleair geladen raketten in de ruimte.

De elektromagnetische puls (EMP) die vrijkomt na een nucleaire explosie stelde de onderzoekers voor grote problemen. Het magnetische veld van de EMP induceert spanning in stroomkringen. Zowel die optredende spanning als de daarmee gepaard gaande stroom kan (hitte-)schade veroorzaken in elektrische bedradingen. Bedradingen en componenten kunnen tegen EMP worden beschermd door deze onder te brengen in een geaarde omgeving (hardening), maar antennes bijvoorbeeld niet.

In de ruimte gestationeerde nucleaire ASAT zijn bijvoorbeeld de *nuclear pumped* ASAT. Deze wapens gebruiken een nucleaire explosie in de ruimte om röntgenstraling, neutronen, gammastralen, of andere straling uit het elektromagnetisch spectrum te genereren en die te richten op de doelsatelliet. Dit zijn enkelschots-wapens omdat de nucleaire explosie het wapen direct vernietigt. Dit soort wapens zijn echter eveneens een gevaar voor de bevolking op aarde, bij gebruik of bij onbedoelde ongelukken, vanwege het naar de aarde dalende radioactieve ruimtepuin dat daar het gevolg van kan zijn. Deze wapens zijn alleen theoretisch onderzocht.

Conclusie

Na de niet voorziene effecten van de EMP zijn Amerika en de Sovjet Unie gestopt met de nucleaire optie voor ASAT. De *Comprehensive Test Ban Treaty* verbiedt sinds 1996 het tot ontploffing brengen van een nucleair wapen in de ruimte. Er is/wordt veel studie verricht naar de mogelijkheden om elektronische apparaten te hardenen (beveiligen) tegen een veelheid aan stralingen. Door steeds betere hardeningstechnieken wordt EMP nu weer gezien als een mogelijke toekomstige optie.

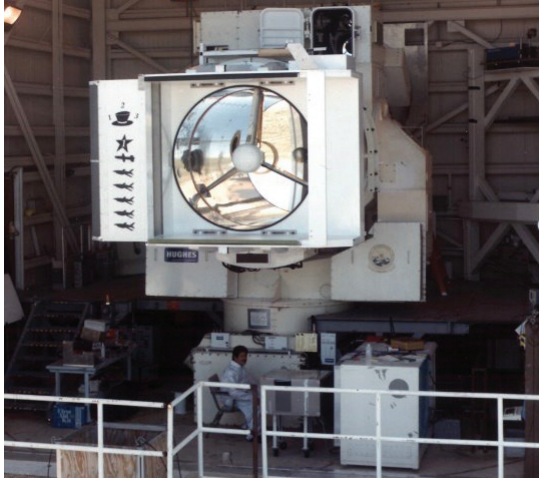
Directed Energy (DE) ASAT

Een *Directed Energy Weapon* (DEW) is een wapensysteem dat schade aan een doel toebrengt door dat doel te bestrijken met gebundelde energie zoals laser-, microgolf- of deeltjesstralen. Een DEW kan worden gebruikt tegen personen, materiaal, en meer specifiek tegen satellieten, waarmee het een DE-ASAT wordt.

Laser

Lasers worden al lang gebruikt tegen doelen in de ruimte en zijn vaak onderdeel van specifieke wapenprogramma's. Een laser is een lichtbron die in staat is een smalle bundel licht voort te brengen waarbij dit licht coherent, monochromatisch en directioneel is. Laagvermogen lasers worden bijvoorbeeld gebruikt voor precieze afstandsmeting, maar ook voor het verblinden van sensoren op satellieten. Aangetoond is dat commercieel verkrijgbare laagvermogen lasers effect kunnen hebben op satellietsensoren. Van Amerika, China en Rusland is bekend dat zij onderzoek doen (en testen bij ABM proeven) naar medium- tot hoogvermogen lasers in het kader van antisatellietwapens. Naar verluid zijn er veel meer landen die onderzoek doen naar militair bruikbare lasersystemen, maar dat is moeilijk aan te tonen.

Laagvermogen lasers kunnen worden gebruikt om missiekritieke satellietsensoren tijdelijk of permanent te verblinden. Een satelliet met een laser aanvallen vanaf de aarde vraagt om eigenschappen als hoge lichtstraalkwaliteit, adaptieve optica (continue aanpasbare spiegels die de turbulentie in de atmosfeer compenseren), en geavanceerde controle over het richten van de laserstraal. Deze technologieën zijn zeer complex en kostbaar, maar haalbaar voor hooggeïndustrialiseerde landen. Ook is een laserstraal pas effectief tegen een satellietsensor als het mogelijk is deze straal binnen het gezichtsveld (*field of view*) van de sensor te richten.



Links: YAL-1 Airborne Laser Test Bed met de spiegel zichtbaar in de neus [US-MDA]. Rechts: MIRACL Mid-Infrared Advanced Chemical Laser Beam Director. [Wikipedia]

Om meer dan de sensoren van een satelliet te verblinden en dus structurele schade toe te brengen, moet het wapensysteem behalve de hiervoor genoemde eigenschappen ook een hoog vermogen (100+ kW) hebben. Er wordt over de hele wereld hard gewerkt aan hoogvermogen lasers voor allerlei toepassingen. Echter, voordat militaire operationele toepassingen met hoogvermogen lasers gemeengoed worden, moeten nog heel wat problemen worden opgelost. Huidige laser wapensystemen zijn te zwaar (vermogen) om sensoren te verblinden en te licht om structureel schade toe te brengen aan satellieten. Chemische lasers zijn de enige systemen die megawatt vermogens kunnen produceren, maar de brandstof die daarbij moet worden gebruikt is zwaar giftig en ze moeten worden gevoed door een externe krachtbron. Elektrisch aangedreven halfgeleider lasers zijn goed te maken en gemakkelijker in het gebruik, maar kunnen (nog niet) voldoende vermogen leveren. Het onderzoek en de ontwikkeling van adaptieve optica vindt voornamelijk plaats in Amerika, Canada, China, India, Japan en Rusland.

Amerika

De meeste DEW lasersystemen worden ontwikkeld voor verdediging tegen (ballistische) raketten maar hebben inherente ASAT mogelijkheden. Voorbeelden in Amerika zijn de *Mid-Infrared Advanced Chemical Laser* (MIRACL) voor de Amerikaanse marine en de Boeing YAL-1 *Airborne Laser Test Bed* (ALTB) voor de luchtmacht. De MIRACL is een *Chemical Deuterium Fluoride Laser* die operationeel werd in 1980. Deze laser kan gedurende 70 seconden een 1 MW ongedempte golf van licht produceren. Oorspronkelijk was deze laser bestemd om op schepen te worden geplaatst ter bescherming tegen *anti-ship* kruisvluchtwapens, maar hij is ook getest tegen ballistische raketten en, in 1997, als ASAT tegen een oude Amerikaanse satelliet (MSTI-3).

De ALTB *Chemical Oxygen Iodine Laser* vernietigde in 2010 met succes ballistische raketdoelen. Het programma werd in 2011 gestopt (kosten $ 5 miljard). Sommige technologieën van de ALTB worden hergebruikt in nieuwe militaire systemen. Het *High Energy Liquid Laser Area Defense System* (HELLADS) dat door DARPA wordt ontwikkeld, heeft met succes gebruik tot 150 kW aangetoond tegen een grote verscheidenheid aan doelen. In Amerika worden natuurlijk nieuwe systemen ontwikkeld, maar de bijzonderheden daarvan worden geheim gehouden en ondergebracht/verstopt in allerlei begrotingsonderdelen. Om een voorbeeld te noemen: *In 2016 Boeing Directed Energy and Strategic Systems was awarded a $275,000,000 indefinite-delivery/ indefinite-quantity contract for research, engineering, and program management to advance scientific and technical knowledge of ground-based space-superiority capabilities and technology, and then apply and transition that knowledge to achieve Air Force and national goals*.

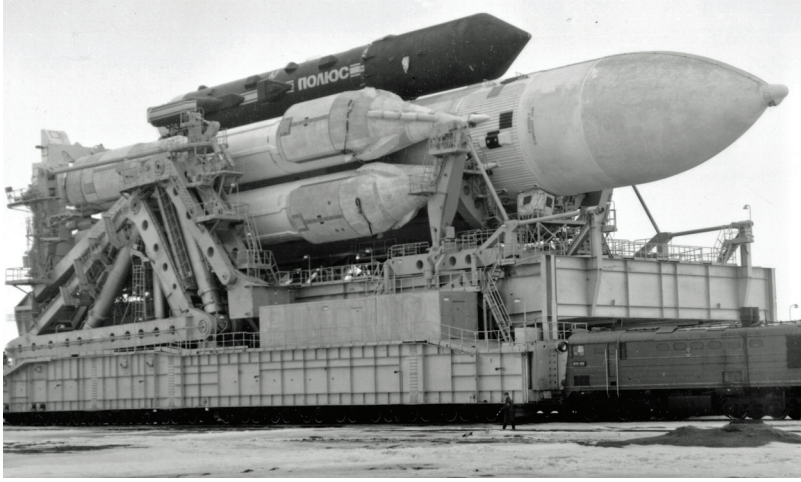
Rusland

Rusland heeft veel academische kennis op het gebied van *directed energy* fysica en ontwikkelt van oudsher allerlei militaire lasertoepassingen. Hieronder vallen bijvoorbeeld vliegtuig- en grondgebonden lasersystemen voor het aanvallen van missiekritieke sensoren en onderdelen in satellieten.

Tijdens de tachtiger jaren begon de Sovjet Unie met een ontwikkelingsprogramma voor het plaatsen van een hoogvermogen laser op een aangepast Il-76 transportvliegtuig (Beriev A-60). De laser werd geïnstalleerd in het vrachtruim met een opening boven op het vliegtuig. Zo werd het Skif-DM lasersysteem getest. Nadat het eerste vliegtuig in een brand verloren was gegaan, werd met een tweede het testen voortgezet. Naar verluidt hebben er verschillende succesvolle testen (2009) plaatsgevonden voordat het programma in 2011 om financiële redenen werd stopgezet. In 2012 werd het programma echter al weer hervat. In april 2017 sprak een vertegenwoordiger van het Almaz-Antey ontwerpbureau dat zij opdracht hadden gekregen *to develop weapons that could interfere electronically with or achieve direct functional destruction of those elements deployed in orbit*. Dit nieuwe systeem wordt Sokol Echelon genoemd en zal worden uitgerust met de 1LK222 laser die afwijkt van de Carbon Dioxide Laser uit de jaren tachtig. Het zou volgens persbureau Tass op een hagelnieuw vliegtuig worden geïnstalleerd. Mogelijk zou dit de nieuwe Tupolev PAK-DA strategische bommenwerper zijn. Van het 1LK222 lasersysteem zijn in het publieke domein geen gegevens bekend.

Rusland heeft een groot aantal (soorten) operationele laser afstandsmeting stations waarvan het merendeel de capaciteit heeft om gevoelige optische sensoren op satellieten (tijdelijk) te verblinden. Van deze laserstations maken negen stuks deel uit van de wereldomvattende *International Laser Ranging Service* (ILRS). Het ILRS netwerk ondersteunt laser afstandsmeting voor geodetisch wetenschappelijk werk met satellieten die daarvoor reflectoren hebben.

Al in de zeventiger jaren ontwikkelde en testte de Sovjet Unie een in de ruimte gestationeerde hoogvermogen laser voor ASAT missies. Het testplatform Skif-DM (Polius) was een uitzonderlijk groot en zwaar ruimtevaartuig (80T) dat alleen maar door de Energia draagraket in de ruimte zou kunnen worden



Links: Beriev A-60/Il-76 Airborne Laser Testbed [Beriev Aircraft Company]. Rechts: Skif-DM/Polius-Energia combinatie op het Baikonoer lanceercentrum [forum.kerbalspaceprogram.com]

gebracht. Deze laser ging verloren in de laatste, mislukte, lancering van de Energia draagraket op 11 mei 1987. Later werd bekend dat de Skif-DM een 1 MW Carbon Dioxide Laser was. Er vonden geen vergelijkbare lanceringen plaats en het programma is hoogstwaarschijnlijk bij het ter ziele gaan van de Sovjet Unie in 1991 beëindigd. Er zijn geen aanwijzingen dat Rusland op dit moment de mogelijkheid/technologie bezit, noch het plan heeft, om een laser ASAT capaciteit in de ruimte te ontwikkelen.

China

China ontwikkelt lasertechnologie sinds de zestiger jaren en maakt er geen geheim van dat zij zich intensief bezighoudt met het ontwikkelen van laserwapens (programma 640-3). Het daaropvolgende programma 863 bestudeerde *Free Electron Lasers* en *Chemical Oxygen Iodine Lasers* die rond 1993 werden getest. China test openlijk laserwapens tegen bijvoorbeeld vliegtuigen en drones en brengt deze commercieel op de markt. Een voorbeeld van een operationele militaire laser in de aanbieding is de LW-30 die in november 2018 op de Zhuhai Airshow werd tentoongesteld.

Wetenschappelijke onderzoekers publiceerden in 2013 in het blad *Chinese Optics* dat China in 2005 een 50 - 100 kW grondgebonden laser heeft gebruikt tegen een satelliet in lage aardomloop (600 km) en in 2006 werd China er van verdacht Amerikaanse satellieten met laser te hebben bestreken. China is een actief lid van de ISLR service en heeft zeven aangesloten laser stations.

Chinese wetenschappers publiceren veel over lucht-, zee- en ruimte gebonden lasers, maar er zijn in het publieke domein geen aanwijzingen dat deze daadwerkelijk worden getest. Mocht China een ruimtelaserplatform ontwikkelen, dan heeft zij wel de mogelijkheid zo'n zwaar platform (5 - 10T) in de ruimte te brengen met hun Lange Mars-5 draagraket.

Hoogvermogen microgolfwapen

Microgolfwapens kunnen door het gericht uitzenden van microgolfenergie schade toebrengen aan een doel en hebben sinds Starfish Prime de aandacht van militairen. De wapens genereren een intense golf van microgolfenergie die sterk genoeg is om elektrische circuits te overbelasten en grote stromen te induceren die tijdelijk dan wel permanent elektrische systemen onklaar maken of zelfs doen smelten. Twee soorten wapens worden onderscheiden. De ene is de elektromagnetische pulsbom (e-bomb); de andere is de z.g. maser (microgolfversterking door gestimuleerde uitzending van straling). Wapens variëren van laagvermogen *Active Denial Systems* die de oppervlakte van het doel verhitten (bijvoorbeeld de huid van mensen als *crowd control* wapen) tot hoogvermogen radarsystemen die vijandelijke elektronica (bijvoorbeeld van UAVs) op afstand onklaar kan maken door via antennes binnen te dringen.

Theoretisch is het probleem onder controle, maar er moeten nog wel een aantal praktische en technologische horden genomen worden voordat het beoogde wapen operationeel als ASAT kan worden ingezet. Te denken valt aan voldoende uitgezonden vermogen en hoge versterking antennetechnologie. Het omzeilen van de beperkingen door de invloed van de atmosfeer (waterdruppels absorberen microgolven) kan worden gerealiseerd door het wapen op een platform (satelliet) in de ruimte te stationeren.

Deeltjesstraling

Een *Partical Beam Weapon* (PBW) gebruikt een hoge energiestraal van geladen of neutrale atomaire of subatomaire deeltjes om schade aan een doel toe te brengen door het verstoren van de moleculaire of atomaire structuur van het doel. Het is de minst ontwikkelde van de DEWs technologieën en krijgt voor zover bekend ook de minste financiering. Het is eigenlijk ook geen echte DEW. Lasers en masers sturen elektromagnetische energie naar het doel. Een PBW brengt kinetische energie naar de atomaire structuur van het doel en is dus eigenlijk een *hard-kill* wapen.

Theoretisch wordt het PBW volledig begrepen en wordt er op kleine schaal, wetenschappelijk, mee geëxperimenteerd. De praktische uitvoering, voldoende energie op het doel krijgen in een militaire conflictomgeving zodat het doel onklaar wordt gemaakt, is verre van realiseerbaar. Het Amerikaanse *Strategic Defense Initiative* ontwikkelde de theorie/technologie van de elektrisch neutrale deeltjesstraal die op een in de ruimte gestationeerd platform zou moeten worden geplaatst. Een prototype van dit wapen werd in 1989 met succes getest tijdens een vier minuten durende sub-orbitale vlucht waarna het uiteindelijk in het Smithsonian Museum in Washington DC belandde. Vooralsnog wordt het PBW nog niet gezien als een praktisch uitvoerbare ASAT.

Conclusie

De drie DEWs die hier zijn besproken zijn de meest bekende. Er zijn nog exotischere wapens zoals het *Laser-Induced Plasma Channel Weapon*, *Pulsed Energy Projectiles*, of het *Long-Range Accoustic Device Weapon* om er maar enkele te noemen. Al dit soort wapens zijn, zeker in Amerika en Rusland, de revue gepasseerd, of heeft men getracht te ontwikkelen en zo mogelijk te testen. Vooralsnog, voor ASAT doeleinden, komen alleen laserwapens in aanmerking. We

Artistieke afbeelding van een Particle Beam Weapon [activistpost.com]

Ruimtevaart en Cyber(on)veiligheid

Drie decennia geleden was *cyberspace* een term uit de sciencefiction literatuur die werd gebruikt om het ontspruitende netwerk van gekoppelde computers aan te duiden. Vandaag de dag is ons moderne leven grotendeels afhankelijk geworden van een goed werkend internet dat in toenemende mate steunt op ruimtevaart gerelateerde communicatie- en informatiediensten en netwerken. Te denken valt onder meer aan kritische infrastructuur zoals nutsbedrijven, communicatie in de meest uitgebreide zin van het woord, financiële en zakelijke dienstverlening zoals telebankieren of betalen met een smartwatch, draadloze controle van kinderspeelgoed tot op afstand bestuurbare/schakelbare elektronische toepassingen, informatie voorziening, meteorologie, defensie, big data, etc. Het merendeel is afhankelijk van ruimtevaart infrastructuur waaronder satellieten, grondstations en dataverbindingen op alle niveaus. Satellietoperaties en andere ruimtevaarttoepassingen vertrouwen in toenemende mate op op het internet gebaseerde netwerken. Inherent hieraan is cyber(on)veiligheid.

Er is een nog niet voltooide vermenging ontstaan van ruimtevaart en cyberspace. Satellieten en andere ruimtevaartmiddelen zijn zoals alle onderdelen van de digitale infrastructuur kwetsbaar voor cyberaanvallen. Cyberkwetsbaarheid manifesteert zich zowel in de aardse infrastructuur (satelliet controlecentra) als in satellieten. Cyberaanvallen op satellieten kunnen de vorm hebben van het storen en/of misleiden (ouderwetse elektronische oorlogsvoering) of van het hacken van communicatienetwerken, maar ook van het tot doelwit maken van satellietcontrolesystemen en missie gebonden software. Mogelijke cyberdreigingen tegen ruimtevaartmiddelen kunnen komen van statelijke- en militaire acties (moedwillige ontwrichting van de maatschappij, verlies van privacy), van georganiseerde misdaad (o.a. *ransomware* om er financieel beter van te worden), niet-statelijke groepen met terroristische motieven (vernietigen van ruimtevaartinfrastructuur) en van individuele hackers die hun kunnen willen showen.

Ruimtevaart is niet meer voorbehouden aan rijke landen met voldoende academische kennis. De huidige technologie brengt ruimtevaart binnen het bereik van landen en (internationale) organisaties, grote bedrijven en zelfs eenlingen. Capaciteiten die een decennium geleden nog strikt waren voorbehouden aan grote inlichtingendiensten zijn tegenwoordig commercieel te verkrijgen. De snelle technologieontwikkeling in de ruimtevaart maakt het haast onmogelijk een passend antwoord te vinden op cyberdreigingen. Bovendien wordt de mensheid geaffecteerd door digitale moeheid (zeker de wat oudere generatie) en houdt de wetgeving geen gelijke tred met de ontwikkelingen.

Technologie op zich kan niet de grondslag zijn voor beleidsontwikkelingen op het gebied van cyberveiligheid. Technologische benaderingen hebben niet de breedte noch de diepte voor volledige deelname van alle stakeholders die bruikbare bijdragen kunnen leveren aan het adresseren van een veelheid aan dreigingen. Het is noodzakelijk een cyberveiligheidsregime te ontwikkelen dat flexibel en multilateraal op de ruimtevaart is gericht. Internationale samenwerking is daarbij een absolute noodzaak. Een niet bureaucratische aanpak moet daarbij standaarden ontwikkelen op het gebied van samenwerking, risicoanalyse, kennisuitwisseling en innovatie om te komen tot een slagvaardig en effectief antwoord op de dreigingen.

Links: Russisch EW systeem [americanmilitaryforum.com]. Rechts: Computer Network Operations [adfind.tv]

zien dan ook dat door een aantal landen, niet alleen Amerika, China en Rusland, verschillende soorten laserwapens worden ontwikkeld.

Electronic Warfare (EW) ASAT

Elektronische oorlogsvoering (EOV) wordt wel gedefinieerd als het toepassen van alle mogelijke processen om het elektronische dataverkeer van de vijand te onderscheppen, verstoren of onmogelijk te maken. In het kader van EW-ASAT praten we dan bijvoorbeeld over het met opzet storen van de vijandelijke radiofrequentie verbindingen van en naar een satelliet. Dit wordt vaak aangeduid met het 'jammen' van de verbindingen. Jamming van de satelliet met een interferentiesignaal wordt het jammen van de 'uplink' genoemd; jamming van het grondstation het jammen van de 'downlink'. Het onderscheppen van deze up- en downlinks i.p.v. ze te jammen kan belangrijke informatie opleveren. EW mogelijkheden en kwetsbaarheden worden beschouwd als zeer gevoelige informatie en daarom is er weinig specifieks bekend in het publieke domein. Testen worden over het algemeen gedaan in speciale omgevingen (Kooi van Faraday) van waaruit geen informatie kan ontsnappen. Wel is algemene theoretische kennis over de mogelijkheden van EW beschikbaar en die kennis is onverkort van toepassing bij dataverkeer tussen satelliet en grondstation v.v.

EW-ASAT is iets dat niet alleen is weggelegd voor Amerika, China en Rusland. Omdat heel veel elektronische datauitwisseling via satellietkanalen gaat, houden landen die regionaal militair iets te betekenen hebben zich hier mee bezig omdat ze weten dat hun tegenstanders het ook doen. Ook Nederland. Zo houdt 102 EOV-compagnie van de Koninklijke Landmacht zich bezig met Elektronische Oorlogsvoering. De compagnie is een onderdeel van 103 ISTAR-bataljon, dat militaire inlichtingen verzamelen tot hoofdtaak heeft. De compagnie houdt zich bezig met het onderscheppen, afluisteren, uitpeilen, analyseren en (ver)storen van radiocommunicatie en andere typen radio-uitzendingen. Echter, het gesproken woord is daarbij al lang niet meer de alles bepalende factor en het accent verlegt zich meer en meer naar interceptie van elektronische signalen die technische informatie bevatten. Het is ondenkbaar dat Nederland militaire missies uitvoert zonder dat een component van EOV wordt toegevoegd.

Cyber Warfare (CW) ASAT

De grens tussen EW-ASAT en CW-ASAT is vaag en soms wat gekunsteld. Ook diverse benamingen die door elkaar heen worden gebruikt scheppen soms verwarring: *Information Warfare, Computer Network Operations, Deception Operations, Cyber Counterspace, Network Centric Warfare, Command & Control Warfare*. Nieuwe technologieën die worden toegepast maken daarbij gewag van *Spectrum Warfare* waarin elektronische- en cyber oorlogvoering, en andere technologische toepassingen om het RF-spectrum te controleren/beheersen, worden samengevoegd. Het zijn *low cost/high value* operaties die grote asymmetrische effecten kunnen hebben. Satellieten voor communicatie en dataoverdracht spelen een cruciale rol hierin. Niet alleen de steeds toenemende technologische vooruitgang, maar ook de brede proliferatie daarvan, is er de oorzaak van dat (commerciële) elektronische verbindingen, bekabeld of niet, gevoeliger worden voor inbraken (hacking) in netwerken. Te denken valt hierbij aan de vele draadloze (wifi) toepassingen zoals handcomputers, mobiele telefoons en zelfs op afstand bestuurbare (video)camera's, gebruikstoestellen en speelgoed. Al deze apparaten, indien niet goed beveiligd, zijn uiteindelijk potentiele ingangen in computernetwerken die worden geëxploiteerd door kwaadwillenden met het doel deze netwerken te controleren/over te nemen. De (data)verbinding via satellieten om netwerken te koppelen is daarbij van het grootste belang (meest gebruikt) en is nog steeds vaak de zwakste schakel. Militaire verbindingen lopen veelal via speciaal beveiligde satellieten, maar netwerkkoppelingen van elektriciteitscentrales en/of andere nutsbedrijven moeten het vaak doen met zwak of niet beveiligde commerciële satellietverbindingen en zijn inherent gevoelig voor inbraken.

Conclusie

EW-ASAT en CW-ASAT zijn hier summier behandeld omdat zij altijd onderdeel van een groter geheel zijn. Men kan de Command & Control van een satelliet overnemen en dus de satelliet laten doen wat men wil, of zelfs uitschakelen zonder ruimtepuin te veroorzaken. Men kan ook inluisteren in de datastroom en daar essentiële informatie uithalen. Of men kan inbreken in de datastroom en zich zo bij een aangesloten netwerk toegang verschaffen. EW-ASAT en CW-ASAT kunnen daarbij zowel in de plaats komen van conventionele *counterspace* operaties of daaraan complementair zijn.

Henk Smid is gepensioneerd hoofdofficier van de Koninklijke Luchtmacht, ruimtevaart analist en publicist van ruimtevaart gerelateerde artikelen.