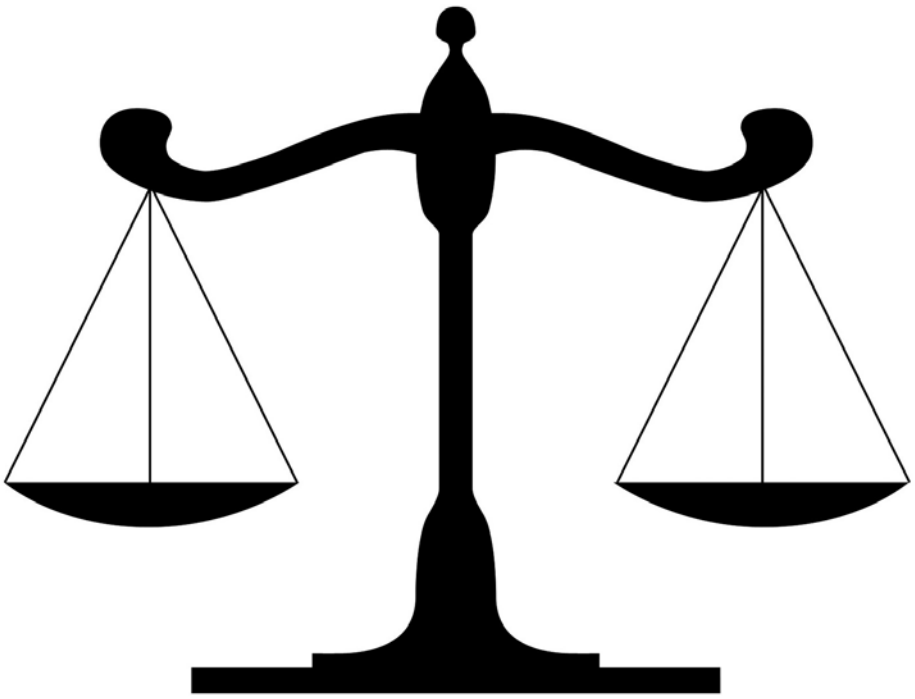
RCIED JAMMERS

Kapitein H.A.C. Wiedeman, DMO/C3I

Tegenstanders hebben tijdens de missies in Irak en Afghanistan in ruime mate gebruik gemaakt van Improvised Explosive Devices (IEDs). 66% van de slachtoffers onder coalitietroepen (2001-heden) is gevallen door toedoen van IEDs is. Het gebruik van IEDs heeft voor opponenten een aantal voordelen; ze zijn relatief simpel, ze kosten weinig en de risico's zijn beperkt.
Er zijn veel soorten IEDs. De IED die ik in dit artikel bespreek is de Remote Controlled IED (RCIED). Deze IED maakt gebruik van zend- en ontvangapparatuur om springstoffen te laten detoneren. Door het gebruik van jammers beschermen we ons tegen deze dreiging.
Ik beschrijf hoe de bescherming met jammers wordt opgebouwd, de hardware en software. Vervolgens ga ik in op de dreiging en het frequentiebeheer en zal ik het hebben over de integratie van jammers binnen het mobiele optreden.

Binnen de krijgsmacht is nog geen uitgebreide ervaring met het gebruik van jammers. We kunnen het uitgestegen personeel en het mobiele optreden voorzien van jammers en zijn intussen bezig om dit gebruik structureel in te bedden in de organisatie. Denk hierbij aan de DCTOMP-factoren (Doctrine, Commandovoering, Training, Organisatie, Materieel, Personeel).
In een ideale wereld kunnen we zelf zonder beperking communiceren en daarbij jammers gebruiken. Maar is dit wel haalbaar? Of gaat de verbetering van de bescherming ten koste van de commandovoering? Omdat onze C2-middelen zich dicht bij de jammers bevinden, storen de jammers ook onze eigen radio's.

> Berichten uit het inzetgebied onderschrijven deze spagaat: "De jammers werken niet". "Jouw jammers storen onze frequenties".
>
> Aangezien een tegenstander waarschijnlijk niet genegen is andere frequenties te gebruiken, moet een oplossing worden gezocht. De jammers werkten prima. Maar de aard van het probleem is helder.



Balans tussen C2 en bescherming.
Beslissen in het gevecht, bouwen aan veiligheid, De ontwikkeling van het landoptreden, Lgen Bertholee, (2008). Teneinde het gehele scala aan opdrachten in het kader van een landoperatie succesvol te kunnen uitvoeren, dienen landstrijdkrachten binnen hun militair vermogen te beschikken over diverse operationele functionaliteiten. Deze vinden hun grondslag in de Essential Operational Capabilities (EOC's), zoals door NAVO opgesteld.

Het doel van de jammers is een optimale bescherming te creëren voor personeel en materieel tegen RCIED dreigingen. Maar hoe moeten jammers worden geïntegreerd binnen het landoptreden zonder dat dit ten koste gaat van de commandovoering?

HARDWARE

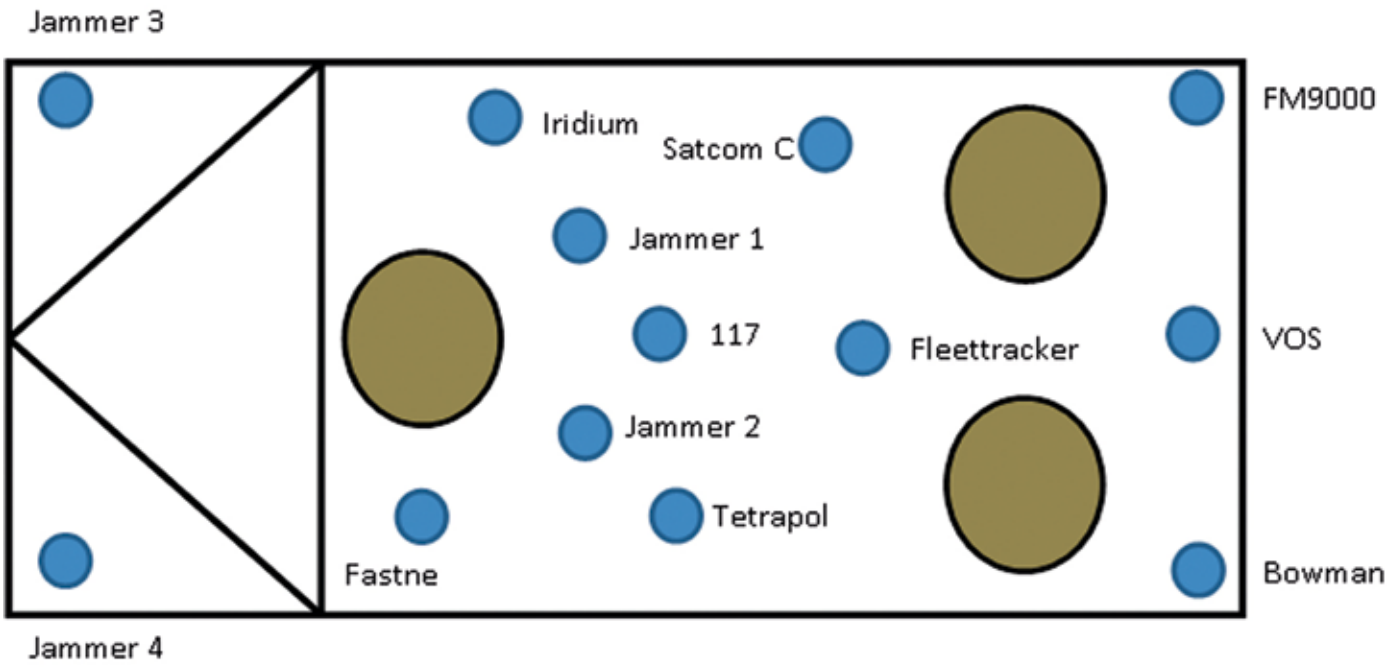
Een jammerconfiguratie bestaat uit: antenne, antennekabel, jammer, stroomkabel, radiorek en eventueel filters. Wanneer een nieuw voertuig moet worden voorzien van jammers worden er eerst specificaties opgesteld, een ontwerp gemaakt en een prototype gebouwd en getest. Als het prototype is goedgekeurd, kan worden gestart met de aankoop en de inbouw van het materiaal. Delen van dit proces kunnen wel parallel worden aangelopen, maar voor de inbouw van een nieuwe voertuigset ben je al snel negen maanden kwijt. Wanneer levertijden voor specifieke onderdelen van een configuratie oplopen tot drie maanden ben je bij het maken van een prototype en vervolgens de verwerving voor de serie al twee maal drie maanden verder. Ervan uitgaande dat het prototype in een keer voldoet. Tijd is dus een belangrijke schakel.

Aspecten die tijd kunnen kosten bij het bouwen van een prototype zijn verder: het maken van een nieuw radiorek, het inbouwen van een nieuwe accu, het aanpassen van kabeldoorvoeren en het vaststellen van de locatie van de antennes op het dak van het voertuig. Op het dak van een voertuig is altijd te weinig ruimte; dit komt omdat we veel antennes kwijt willen op een voertuig. Naast de antennes van de C2-appratuur en jammers moet er ook rekening worden gehouden met andere constructies die op het dak worden gemonteerd (bv opbergrekken, affuiten of een reservewiel).

Voor een bepaalde periode wordt een standaard jammerconfiguratie vastgesteld. Er is geld beschikbaar in het DIP (Defensie Investerings Plan) om onderzoek te doen naar ontwikkelingen en te kunnen vaststellen welke configuratie nodig is om op de dreigingen in een bepaalde periode te kunnen anticiperen. Door de vaststelling van een standaardconfiguratie wordt al veel tijd bespaard.

SOFTWARE

De software van de jammer bestaat uit twee delen. Als eerste hebben we de firmware: de firmware zorgt er voor dat de jammer ge-



Mogelijke schematische weergave van de plaatsing van antennes op een voertuig

bruiksklaar is. Bij de firmware is versiebeheer vooral belangrijk, omdat deze compatibel moet zijn met de laadapparatuur. Maar het belangrijkste deel van de software is de 'jamfile'. De jamfile vertelt de jammer op welke frequentie, op welk vermogen en met welk interval hij moeten zenden. Omdat je ook een interval kunt instellen, kun je met een jammer meerdere dreigingen storen, of je laat ruimte om zelf met C2-apparatuur te zenden.

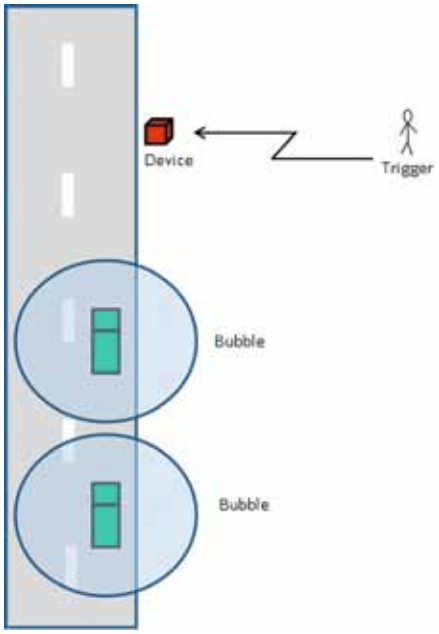
Idealiter wil je dus met een jammer zoveel mogelijk dreigingen storen. Daarom is het belangrijk om per dreiging te weten hoe lang je de dreiging moet storen (dwell time) en hoe snel je moet terugkeren (revisit time) op die frequentie zonder dat de RCIED afgaat. Bij de tijden die worden ingesteld bij de dwell time en revisit time moet men denken aan milli- en microseconden. Het vaststellen van de combinatie minimale dwell time en revisit time en vermogen is specialistisch en arbeidsintensief werk.

De gevolgen van een te laag vermogen of te korte dwell time zijn evident. Hoe minder de jammers zenden hoe minder last de C2-apparatuur er van heeft.

DREIGING

Een RCIED maakt dus gebruik van een zender en een ontvanger. De zender noemen we de 'trigger' en de ontvanger het 'device'. Het device is verbonden aan een ontsteker en explosieven. Jammers voorkomen dat het device afgaat.

De jammers storen de verbinding tussen de trigger en het device en creëren een veilige ruimte, ook wel de 'bubble' genaamd. Als het device zich in een bubble bevindt kan het niet door de trigger worden geactiveerd, dat kan gebeuren omdat er meer vermogen van de jammer binnenkomt bij het device dan van de trigger. Of de jammer kan op een slimme manier voldoende signaal verstoren. Bepaalde communicatieapparatuur kan geen verbinding maken als je al 25% van de tijd het signaal verstoort.



Voertuigen met bubble

FREQUENTIEBEHEER

De dreiging bepaalt dus welke frequentie moet worden gestoord. Per land of regio is dit verschillend. Goede informatie over de dreiging is cruciaal. Omdat de tegenstander geen rekening houdt met ons eigen frequentiegebruik, is het belangrijk dat er binnen de eigen staf wordt gecoördineerd. Als de profiler (verantwoordelijk voor de jamfile) binnen de sectie 3 werkzaam is, moet dit worden besproken binnen de secties 2,3 en 6. De dreigingsinformatie moet uit de lijn van de sectie 2 komen en de sectie 6 is verantwoordelijk voor het frequentiebeheer van de eigen systemen. Behalve de eigen C2-systemen op het voertuig kunnen ook andere systemen in de omgeving van de jammer last hebben. In Nederland is het spectrum bijna volledig bezet en ook al heeft het bestrijden van een dreiging prioriteit, je wilt wel weten wat de invloed daarvan is op bijvoorbeeld de aansturing van vitale infrastructuur of de communicatie op een vliegveld. Je kunt voor specifieke locaties dus al een spectruminventarisatie doen. Het kiezen van de eigen frequenties is dan ook belangrijk en afhankelijk van de dreiging en de omgeving. Het kan ook zijn dat de dreiging gebruikt maakt van dezelfde frequentie als de eigen de C2-apparatuur. De commandant van een voertuig kan dan besluiten om wel of niet een jammer te gebruiken. Als de omgeving rond een voertuig is veilig gesteld en er verbinding nodig is kan de jammer worden uitgezet; dit vereist wel een bepaald bewustzijn en kennisniveau bij de gebruiker.

INTEGRATIE

Zoals gezegd worden prototypes en wijzigingen aan het voertuig getest. Er moet worden zeker gesteld dat de afstraling van het voertuig voldoende is en de configuratie voldoet aan de eisen. Personeel van LCW draagt zorg voor deze testmetingen. Omdat propagatie en antennetechniek niet altijd heel voorspelbaar zijn, zijn deze testen dus belangrijk. Wijzigingen aan een voertuig kunnen heel divers zijn en dus een nieuwe test tot gevolg hebben. Voorbeelden zijn: 'Extra metaal op dak' (affuiten, kijkers, rekken) of extra C2-apparatuur. De jamfile en de C2-middelen moeten ook opnieuw worden getest als de frequentie van een van beide wijzigt of als er nieuwe dreiging bij-

komt. Door het gebruik van filters kunnen we de stoorsignalen ook redelijk afschermen van de eigen C2-middelen. Het wijzigen van frequenties kan betekenen dat er ook nieuwe filters moeten worden aangekocht en ingebouwd. Het testen van een nieuwe jamfile en het wijzigen van een constructie kan worden gecombineerd. Op dit moment is binnen DMO de verantwoordelijkheid van een voertuig en de communicatieapparatuur binnen verschillende directies belegd, nl. MATLOG en JIVC. Tot voor kort zaten ook niet alle projectmanagers van radiosystemen in een afdeling.
Gebundelde kennis over frequentiegebruik door de huidige en toekomstige C2-middelen en de te verwachten dreiging is essentieel. Hiervoor bevinden zich bij de JTF-CIED stafcapaciteit en een profiler. De profiler is een aanspreekpunt voor de brigadefunctionarissen en verantwoordelijk voor het maken van jamfiles, hierin kan hij worden ondersteund door TNO. Omdat het inzetgebied divers kan zijn en ad hoc een jamfile nodig kan zijn, is het belangrijk dat medewerkers van TNO zich permanent kunnen richten op dit onderwerp. Zij kunnen ook extra onderzoek doen naar een nieuwe dreiging of probleem. Hier moet dan wel budget voor zijn.

TOT SLOT

Als we kijken naar de jammerconfiguratie kunnen we stellen dat de huidige configuratie vrij uitgebreid is en een breed scala aan dreigingen kan storen. Er is ook geld aanwezig om periodiek onderzoek te doen naar ontwikkelingen en om te bekijken of de configuratie nog voldoet. Enig nadeel is dat de huidige configuratie nog vrij veel antennes nodig heeft. Dit is een probleem bij veel voertuigen omdat er eenmaal weinig ruimte is. Jammers van een volgende generatie kunnen dit misschien verhelpen. Andere opties zijn: werken met combiners of dreigingen reactief bestrijden.

Voor het maken van de jamfile hebben we een profiler. Naast de profiler komen er ook functionarissen op brigadeniveau die zich kunnen gaan bezighouden met RCIED-jammers. Het maken van een jamfile is heel complex, zeker als je op korte termijn voor een bepaalde inzet in een bepaald gebied een jamfile moet maken.
De ontwikkeling van nieuwe dreigingen zijn niet allemaal door een man bij te houden, immers elke zender/ontvanger kan worden gebruikt voor een RCIED. Het spectrum is dan vrij breed. Ook de complexiteit van bijvoorbeeld LTE is groot. Voor deze kennis kunnen we op dit moment terugvallen op TNO. Structureel zou hiervoor exploitatiebudget beschikbaar moeten zijn om de kennis op peil te houden en indien nodig snel input te geven voor een nieuwe jamfile. Het budgetteren van een ondersteuning die je op onbekende momenten nodig hebt is lastig.

Ondanks dat er een vaste jammerconfiguratie is, is dit nog geen oplossing voor de integratie met de C2-middelen, deze integratie kost tijd. Er zijn binnen de krijgsmacht nog veel onderdelen met verschillende C2-middelen, dus hoe minder verschillende C2-middelen hoe minder combinaties er kunnen zijn met de jammerconfiguraties. Ook de toegewezen frequenties kunnen per gebied verschillen. Dit kan worden verholpen met filters en/of afstemming binnen secties 2,3 en 6. De sie 2 heeft kennis van de dreiging. De profiler (sie 3) maakt de jamfile. De sie 6 is verantwoordelijk voor het frequentiebeheer en het plannen van de eigen C2-middelen. Bij de planning van de eigen C2-middelen is altijd wel ruimte om slim gebruik te maken van het spectrum. Dit geldt ook voor een jamfile. Niet alle dreigingen hebben bijvoorbeeld veel vermogen nodig om te worden gestoord.
Het uitrusten van een nieuw voertuig met jammers kost tijd. De configuraties voor de meest gangbare voertuigen, die worden gebruikt voor missies, zijn inmiddels wel ontwikkeld. De implicaties van het wijzigen van de samenstelling van de C2-middelen of dakconstructie worden nog onderschat. Het toevoegen van bv een BOWMAN HF-radio aan een Bushmaster zorgt er voor dat het voertuig weer opnieuw moet worden getest. De inbouwploeg en meetploeg van LCW moeten worden ingeschakeld. Er moet waarschijnlijk extra materiaal worden gekocht. Voordat een besluit wordt genomen over aanvulling of aanpassing zou je moeten bekijken wat de implicaties zijn op de jammers en de C2-middelen.
Het bijhouden van de wijzigingen en de integratie van de C2-middelen met de jammers zou kunnen worden belegd bij de afdeling Informatiemanagement en architectuur (JIVC), deze heeft contact met de Defensiestaf en de OPCO's en intern JIVC met de betreffende project- en systeemmanagers.

Kunnen we nu stellen dat de bescherming tegen RCIEDS ten kost gaat van de commandovoering? Ik denk van niet, maar dan moet er wel voldoen worden aan een paar voorwaarden. Voor het uitrusten van een nieuw voertuig is tijd nodig. Gewenste wijzingen door de gebruikers (OPCO/CDS) moeten worden gecoördineerd. Daarmee bedoel ik dat de consequenties en haalbaarheid worden duidelijk gemaakt voordat er een besluit wordt genomen. Binnen een staf moeten de dreigingen, C2-plannen en jamfiles op elkaar worden afgestemd. Ook moet er capaciteit worden gereserveerd voor het flexibel en snel optreden kunnen tegenover dreigingen.

Een aantal zaken is niet aan de orde zijn gekomen, dat komt niet omdat ze niet belangrijk zijn maar het is wel te veel om te noemen in dit artikel. Onderwerpen waar we zeker mee bezig en die ik toch wil noemen zijn:
- Manpack jammers (gevolgen voor het uitgestegen optreden).
- Personal jamming (voor- en nadelen tov manpacks op groepsniveau).
- Radhaz (wetgeving en invloed op personeel).
- Herstel- en profilingcapaciteit in missiegebied.
- Diverse modulatievormen.
- Inzet jammers bij partnerlanden.
- Waar vallen jammers onder? (EOV, radio's, bescherming).
- Switch box (actief jammers op voertuigniveau aan/uit zetten).
- Opleidingen (gebruikers, kerninstructeurs, functionaris op brigadeniveau).
- Toekomstige ontwikkelingen.
- Reactief jammen !!!.

Jammervoertuig