Tekst: Rudi Gouweleeuw, TNO Military Operations

Cyber fires?

De Nederlandse krijgsmacht heeft in 2012 een Cyber Strategie[1] opgesteld. In deze strategie wordt de ambitie uitgesproken om de komende jaren de digitale weerbaarheid te versterken en het vermogen te ontwikkelen om offensieve cyberoperaties uit te voeren met als doel de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen. Met een dergelijk cybervermogen heeft een commandant een nieuwe effectenbrenger ter beschikking. Maar hoe zet je zo'n digitaal vermogen, in samenhang met andere vermogens, in?

Tijdens het experiment *Bold Quest* 13.2 is afgelopen september een proef gedaan om een aanvalsactie van een compagnie te ondersteunen met cybercapaciteiten, waarbij cyber werd beschouwd als een speciaal "vuur", conform de reguliere vuursteunprocedures en organisatielijnen. Welke observaties zijn gedaan en welke lessen kunnen daaruit worden geleerd?

Bold Quest

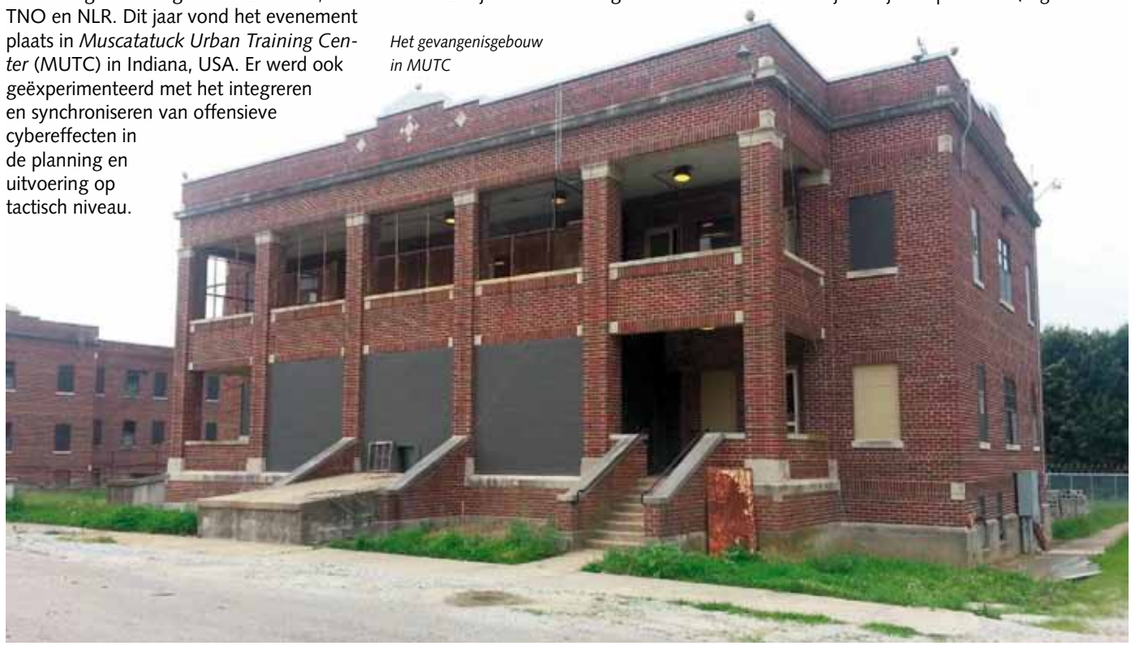
Bold Quest is een experimentenreeks waarin de nadruk ligt op het testen van concepten, middelen en procedures op het gebied van Grond-Lucht samenwerking en *Combat Identification*. Nederland neemt aan deze experimenten al enkele jaren deel met vertegenwoordigers van Defensie, TNO en NLR. Dit jaar vond het evenement plaats in *Muscatatuck Urban Training Center* (MUTC) in Indiana, USA. Er werd ook geëxperimenteerd met het integreren en synchroniseren van offensieve cybereffecten in de planning en uitvoering op tactisch niveau.

TNO voert voor Defensie een cyber onderzoeksprogramma uit en in dat kader heeft de schrijver van dit artikel dit experiment bijgewoond.

Opzet van het cyberexperiment

In Muscatatuck Urban Training Centre staat als één van de ca 100 objecten een gevangenis. Het gevangenisgebouw heeft een kelder en twee verdiepingen en is omringd door een hekwerk. Op elk van de 4 hoeken van het hek staat een videocamera zodat de directe omgeving van de gevangenis geobserveerd kan worden. In het gebouw zijn over de 3 etages 16 videocamera's geplaatst die een overzicht geven van de verschillende ruimtes in het gebouw. Er zijn 25 deuren uitgerust met een sensor (open/dicht) en deze deuren kunnen op afstand geopend en gesloten worden. De deursensoren laten een alarm afgaan als ze ongeautoriseerd worden geopend. De camerabeelden, sensoren en deuren kunnen worden gemonitord en aangestuurd vanuit de gevangeniscentrale op de begane grond. Tenslotte is er een intercom in het gebouw aanwezig.

Het gevangenisgebouw in MUTC



Het geplande scenario was dat er enkele gevangenisbewaarders aanwezig zouden zijn, maar geen gevangenen. De gevangenisbewaarders waren de irreguliere vijand gunstig gezind, waardoor die *insurgents* op een bepaald tijdstip de gevangenis gebruikten als een ontmoetingsplaats van twee vijandelijke kopstukken (*High Value Individuals (HVI)*), met hun lijfwachten. In totaal waren er op dat tijdstip ongeveer 12 personen in het gebouw aanwezig.

Een *BLUEFORCE* brigade was op de hoogte van deze ontmoeting en ging de gevangenis aanvallen om de HVIs gevangen te nemen of uit te schakelen. De actie werd gepland door een brigadestaf en uitgevoerd door twee infanteriepelotons. *BLUEFORCE* was zeer gedetailleerd op de hoogte van de functionaliteit en inrichting van het gebouw en heeft dat via cyberondersteuning uitgebuit.

Cybereffecten

Ruim voorafgaande aan de actie heeft een *BLUEFORCE* cyberteam op afstand digitaal ingebroken in de gevangenis en enkele systemen geruisloos aangepast, zodat tijdens de actie van de volgende cybereffecten gebruik kon worden gemaakt:

1. camerabeelden: meekijken met alle camera's en bovendien per camera het beeld bedienen (camera draaien of in-zoomen), het beeld bevriezen of de camera deactiveren;
2. automatische deuren: per deur open of op slot doen;
3. alarm: alarm initiëren (dus vals alarm activeren) of juist deactiveren;
4. intercom: meeluisteren, deactiveren.

Tijdens de actie zat het cyberteam op een eigen locatie van waar zij de afgetapte beelden konden bekijken, de intercom konden afluisteren en de cybereffecten konden aansturen. De cybereffecten werden ingezet voor 2 doelstellingen:

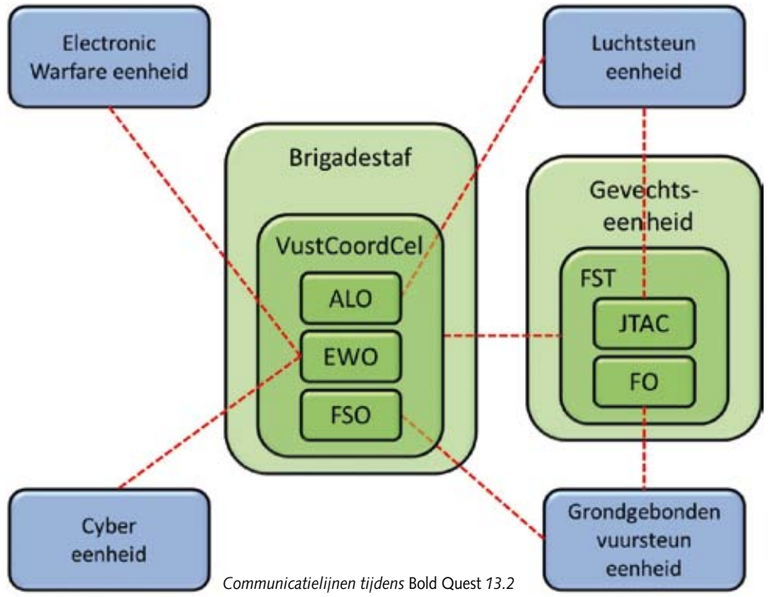
1. verkrijgen van inlichtingen over de toestand en positie van de vijand tot vlak voor de aanval;
2. ondersteunen van de aanval door het ontnemen van *situational awareness* van de vijand (camerabeelden manipuleren) en het verschaffen van toegang (openen van deuren).

Doctrinaire achtergrond / communicatielijnen

Amerikanen hanteren een zeer brede definitie van *Fires*[2], namelijk het gebruik van een systeem om een effect te creëren. In dat kader is het dus ook niet vreemd, dat zij de cybereffecten benaderden vanuit de gedachte dat een cyber effect een *fire* is. Dit uitte zich zowel in de gebruikte terminologie als in de communicatielijnen: tijdens de uitvoering van de tactische actie communiceerde het cyberteam met de *Electronic Warfare Officer* (EWO) van de brigadestaf. De brigadestaf, hetzij de *Fire Support Officer* (FSO) of de EWO zelf, communiceerde met de *Forward Observer* (FO) van de gevechtseenheid die de actie uitvoerde.

Uitvoering van het experiment

Vlak voor de actie kreeg het cyberteam de opdracht om het alarm in de gevangenis aan te zetten om verwarring te stichten en om te zien hoe de vijand zou reageren.



Communicatielijnen tijdens Bold Quest *13.2*

Veel verwarring leverde dit overigens niet op, anders dan dat de vijand het als een waarschuwing voor een aankomende gebeurtenis interpreteerde. Daarna werd de opdracht gegeven alle camera's zowel binnen als buiten de gevangenis te bevriezen, zodat de bedienaar in de gevangenis niet kon zien wat er live gebeurde. Direct aansluitend reed één peloton met hun voertuigen het gevangenisterrein op, stopte voor de deur van de gevangenis en ging door de voordeur naar binnen. Het tweede peloton zorgde voor de rondom beveiliging. Na ongeveer één minuut kwam de opdracht van het eerste peloton om alle deuren op de begane grond in de gevangenis te openen. Na ongeveer 10 minuten kwam de opdracht om de camera's weer te activeren, omdat het peloton de eerste verdieping in handen had en de eerste HVI had uitgeschakeld, maar wilde weten waar de tweede HVI zich in het gebouw bevond. Middels de camera's werd hij opgespoord (hij had zich teruggetrokken in de kelder) en overmeesterd.

Observaties / discussie

Het zal geen verrassing zijn dat de cybereffecten een waardevolle toevoeging waren op het arsenaal dat de aanvallende eenheid ter beschikking had. Het cyberexperiment was hier namelijk op ingericht. Niettemin heeft het experiment belangrijke inzichten opgeleverd of benadrukt, zeker als we een vergelijking maken met de traditionele vuursteun:

- De inzet van vuursteun resulteert in zichtbare effecten in de omgeving (rook, licht, fysieke beschadiging door druk, scherven of brand). Cybereffecten kunnen in de operationele omgeving zichtbaar zijn (zoals bijvoorbeeld het openen van een deur), of juist onzichtbaar (zoals bijvoorbeeld het meeluisteren op de intercom). In het algemeen kunnen cybereffecten ingedeeld worden in drie categorieën: het aantasten van de beschikbaarheid van een functie (een camerabeeld valt uit), het aantasten van de normale werking van een functie (een camera doet het nog wel, maar iemand anders kan het beeld manipuleren) en het aantasten van de vertrouwelijkheid van gegevens (iemand anders kijkt of luistert onopgemerkt mee).
- Vuursteuneffecten kunnen permanent zijn (bijvoorbeeld de fysieke vernietiging van een wapensysteem) of tijdelijk (bijvoorbeeld rook en licht). Zo ook kunnen cybereffecten een permanente verandering in de operationele omgeving zijn (bijvoorbeeld het fysiek beschadigen van

apparatuur door het controlemechanisme te manipuleren, zoals *Stuxnet* dat deed met de uraniumverrijkingscentrifuges in Iran), of een tijdelijke verandering (bijvoorbeeld het bevriezen van een camerabeeld).
Afhankelijk van de eigenschappen van cybereffecten kan er een *Time on Target* en/of een *Time Window* (vergelijk *jamming*) voor het effect worden gedefinieerd.

- Vuursteuneffecten hebben een lokale uitwerking. Cybereffecten daarentegen kunnen een lokale verandering zijn (zoals het uitschakelen van een specifieke camera) maar ook een globale verandering (het uitschakelen van alle camera's die op het wereldwijde internet zijn aangesloten).
- Net als bij vuursteun kunnen cyberactiviteiten ook ongewenste (neven)effecten hebben, er is dan sprake van *collateral damage* (zoals het ongecontroleerd verspreiden van de *malware*). Daarom is de beslissingsbevoegdheid over het inzetten van cybermiddelen afhankelijk van de verwachte soort en omvang van de gevolgen, een juridisch kader en de noodzakelijke synchronisatie met andere effecten. Voor sommige cybermiddelen zou het besluit over inzet bij een operationele commandant kunnen liggen (zoals het geval was in het *Bold Quest* experiment), terwijl voor andere cybermiddelen deze op nationaal niveau kan liggen (zoals dat waarschijnlijk voor *Stuxnet* het geval is geweest).
- Wanneer cybereffecten worden ingezet in het kader van een tactische operatie, heeft de commandant van de gevechtseenheid behoefte aan een functionaris om cybereffecten aan te vragen en de uitwerking daarvan te observeren. In geval van cyber is dat niet noodzakelijkerwijs dezelfde persoon. Sterker, in geval van cyber kan zich een situatie voordoen waarin de cyber *shooter* tevens de cyber *observer* is, en de aanvrager het effect (nog) niet ziet. In het *Bold Quest* experiment bijvoorbeeld initieerde het cyberteam de effecten en kon de resultaten daarvan ook direct waarnemen (zoals het bevriezen van de camerabeelden), terwijl dit niet waarneembaar was voor de gevechtseenheid. Andere cybereffecten waren wel waarneembaar voor de gevechtseenheid, zoals het elektronisch openen en sluiten van deuren. Er zijn zelfs cybereffecten die ook voor de cyber *shooter* niet direct zichtbaar zijn, maar die zich pas veel later en indirect manifesteren, zoals een virus dat geruisloos en onzichtbaar zijn werk doet.
- In het *Bold Quest* experiment fungeerde de brigadestaf als coördinatiecel tussen de gevechtseenheid en het cyberteam: de FO zond zijn cybervuuraanvraag naar de EWO, die vervolgens opdracht gaf aan het cyberteam. De resulterende effectmelding verliep van het cyberteam via de EWO naar de FO. Ook de waarnemingen die het cyberteam deed middels het aftappen van de camerabeelden en de intercom werden via de EWO aan de FO doorgegeven. De timing van deze communicatie is echter dermate cruciaal, dat elk tussenstation vertraging en dus risico oplevert. Gegeven deze tijdkritische coördinatie is het essentieel dat de FO direct kan communiceren met het cyberteam, zoals een FO of JTAC dat ook doet met de vuursteuneenheid.
- Het cyberteam had geen inzicht in het plan van de gevechtseenheid. Daardoor kon het alleen reactief optreden en was het afhankelijk van de opdrachten van de uitvoerende eenheid. Het cyberteam had echter een actuele en superieure inlichtingenpositie en moest soms nagelbijtend en scheldend toekijken terwijl het bijvoorbeeld een HVI de toegang tot een ruimte had kunnen ontzeggen.
- De wijze van inzet van cybereffecten moet goed worden afgewogen. In het *Bold Quest* scenario werden de camera's gedurende het grootste deel van de actie uitgezet om de vijand geen zicht te geven op de activiteiten van *BLUEFOR*. Echter, wanneer de vijand eenmaal doorheeft dat er een aanval plaatsvindt, zouden de camera's ook weer aangezet kunnen worden, omdat het vergroten van de eigen inlichtingenpositie (waar zit de vijand en wat doet hij?) zou kunnen opwegen tegen het feit dat de vijand ook kan zien waar de *BLUEFOR* eenheden zitten. Tijdens het experiment werden de deuren ontgrendeld om *BLUEFOR* toegang tot het gebouw te geven. Maar bepaalde deuren hadden op specifieke momenten gesloten kunnen worden om de bewegingsvrijheid van de vijand te beperken.
- Naast de vuursteuncommunicatielijnen werd ook gebruik gemaakt van standaard vuursteunterminologie. Voor de cybereffecten voldeed deze standaard niet altijd even optimaal en was klare taal vaak duidelijker en sneller geweest. Zo was voor elke camera, deur, alarm en intercom een target nummer gedefinieerd. In plaats van het opsommen van targetnummers was het bijvoorbeeld efficiënter geweest om gewoon te zeggen "bevries alle camera's op de eerste verdieping" of "sluit alle toegangen tot ruimte X af". Ook de terugmelding van het effect zou duidelijker kunnen. Nu werd zowel het aan- als het uitzetten van een camera met *splash* gemeld.
- Een veel geuite wens was de behoefte aan een Cyber Video *Downlink*, de uitvoerende eenheid zou graag willen zien wat de cyber *shooter* ziet. Met een video verbinding wordt trouwens al uitvoerig geëxperimenteerd in het vuursteundomein.

Afsluiting

De inzet van cybermiddelen kent gelijkenissen maar ook verschillen met de inzet van vuursteunmiddelen. Net als andere effecten moeten cybereffecten gepland en gesynchroniseerd worden in het commandovoeringproces. Of de vuursteunketen de meest geschikte lijn is om cybereffecten te coördineren is de vraag. Uit dit experiment is in ieder geval duidelijk geworden dat offensief gebruik van cybercapaciteiten een waardevolle aanvulling is op het arsenaal dat een commandant ter beschikking staat, ook op tactisch niveau. Kanttekening hierbij is dat er nauwelijks een generiek cyberwapen bestaat dat van de plank ingezet kan worden, afgezien van een *Denial of Service* (DoS) aanval. In het *targeting* proces wordt bepaald welk specifiek effect op een specifiek target benodigd is en vaak zal daartoe een speciaal cyberwapen ontwikkeld moeten worden. Dat kost tijd en vergt specifieke expertise.
Het vormgeven van cybercapaciteiten, opleiding en training, een cyberdoctrine en de inbedding daarvan in de Defensie organisatie is een taak van de *Task Force* Cyber. Het uitvoeren van en deelname aan experimenten zoals *Bold Quest* leveren een zinvolle bijdrage aan de daarvoor noodzakelijke kennisontwikkeling.

Voor meer informatie:

Ikol Marco Verhagen, Task Force Cyber, Stafofficier Cyber Operations, JPG.Verhagen@mindef.nl
Rudi Gouweleeuw, TNO programmaleider Defensie onderzoeksprogramma Cyber Operations, rudi.gouweleeuw@tno.nl

Eindnoten

1 *Defensie Cyber Strategie, Ministerie van Defensie, 27 juni 2012*
2 *To employ fires is to use available weapons and other systems to create a specific lethal or nonletal effect on a target. JP 3-0 Joint Operations, 11 August 2011*