TOOLS EN TECHNIEKEN VOOR OFFENSIEVE CYBEROPERATIES

Prof dr. Tim Grant, Faculteit Militaire Wetenschappen, NLDA

Sinds de oprichting van de Nederlandse Defensie Academie (NLDA) in november 2005 is haar Faculteit Militaire Wetenschappen (FMW) verantwoordelijk voor de initiële academisch opleiding van cadetten en adelborsten van alle krijgsmachtdelen. De FMW biedt drie wetenschappelijke bachelors, geaccrediteerd volgens Europese regelgeving. Er is een Bachelor Krijgswetenschappen, een Bachelor Militair Bedrijfswetenschappen, en een Bachelor Militaire Systemen & Technologieën. Met de publicatie van de Nationale Cyber Security Strategie in februari 2011 kan het niet anders zijn dan dat cyberoperaties behandeld moeten worden in alle drie de bachelors.

Om erkend te kunnen worden als wetenschappelijke bachelors (d.w.z. WO i.p.v. HBO bachelors) moet zo'n 50% van de FMW-docenten gepromoveerd zijn en actief bezig zijn met wetenschappelijk onderzoek. De docenten zijn gemiddeld 30% van hun tijd bezig met onderzoek; daarnaast heeft de FMW een aantal AiO's (civiele studenten die bezig zijn met PhD onderzoek) in dienst. In vergelijking met TNO en civiele universiteiten heeft de FMW een aantal "unique selling points": wij doen onderzoek dat én fundamenteel én toegepast is, multidisciplinair is, en gericht is op Defensiebehoeften en -vraagstukken. Uiteraard is cyber nu een "hot topic". Collega's zijn nu al bezig met de operationele en juridische aspecten van cyberoorlogsvoering, met de rol van *social engineering* en sociale media in cyberoperaties, met het modelleren van (C2) netwerken op basis van netwerk- en speltheorie (de harde wiskunde), en met counterintelligence in cyberoperaties.

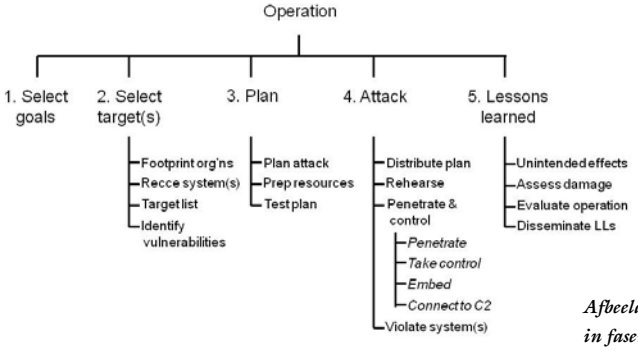
C2 VAN CYBEROPERATIES

Mijn eigen onderzoek gaat over de C2 van cyberoperaties. Ik richt me vooral op het creëren van kennis die nuttig zou kunnen zijn voor de oprichting van het Defensie Cyber Centrum. Juist daarom houd ik me volledig bezig met offensieve cyberoperaties. Er zijn vier soorten offensieve cyberoperaties geïdentificeerd:

- *counter-attack,*
- *pro-active defence (pre-emptive),*
- *directe aanvallen zonder kinetische actie en*
- *directe aanvallen met kinetische actie.*

Er zijn ook goede wetenschappelijke redenen om offensieve cyberoperaties te bestuderen: er is daarover heel weinig gepubliceerd in de openbare wetenschappelijke literatuur. Voor een wetenschapper is onderzoek over offensieve cyberoperaties dus een "target-rich environment".
Op dit moment ben ik bezig met hoe een cyberaanvalproces verloopt, als verlengstuk van de scriptie van Daan Dreijer. Naast Daan's model, heb ik nog zes modellen kunnen vinden in de (semi-) wetenschappelijke literatuur. Met behulp van *Structured Design & Analysis Technique* (SADT, ook bekend als IDEF0) heb ik iedere model geformaliseerd. Daardoor kon ik de modellen met elkaar vergelijken, en een zogenaamd *canonical* ("best of practice") procesmodel van vijf fasen opbouwen (Afbeelding 1). Daarbij heb ik hulp gekregen van twee *subject matter experts* (lees: ervaren hackers) van het *Council for Scientific and Industrial Research* (CSIR, het Zuid-Afrikaanse equivalent van TNO). Wij hebben onze onderzoek beschreven in een paper die nu geaccepteerd is voor het 7e *International Conference on Information Warfare and Security* (ICIW) in maart 2012.

Bij het opbouwen van het canonical procesmodel heb ik nadrukkelijk rekening gehouden met de mogelijkheid om cyberoperaties te synchroniseren met kinetisch actie. Daarom ziet het procesmodel er op faseniveau heel conventioneel eruit. De verschillen zijn te vinden op een lager niveau, vooral in fasen 2, "Select target(s)". en 4, "Attack". Ook de taakverdeling in een professionele offensieve cyber team is bepalend geweest. Ik ga er vanuit dat fase 1, "Select goals", een taak is voor politici, fase 2, "Select target(s)", voor de (militaire) inlichtingen, fasen 3 en 4 respectievelijk voor de militaire planners en *cyberoperatives*, en fase 5 voor het hele team.



Afbeelding 1: Offensieve cyberoperatie in fasen, sub-fasen, en sub-sub-fasen.

WAAROM ZOU EEN DERGELIJK PROCESMODEL NUTTIG KUNNEN ZIJN VOOR DEFENSIE?

In eerste instantie helpt een procesmodel bij het inrichten van het Defensie Cyber Centrum. Het laat zien dat cyberoperaties een samenspel is tussen politici, de inlichtingdiensten, en Defensie. Dit samenspel moet geolied zijn want een counterattack moet in uren, zo niet in minuten of in seconden kunnen reageren op een inkomende aanval. De processen moeten grotendeels geautomatiseerd zijn, en het Defensie Cyber Centrum moet alle tools en technieken ter beschikking hebben. Er is veel meer dan de bekende *malware* nodig. Collaboratie tools (sociale media?) moeten het samenspel faciliteren. Een simulatieomgeving ("cyber test-range") is essentieel, zowel voor het testen van het aanvalsplan in fase 3 als voor *mission rehearsal* in fase 4. In een tweede, korte *paper* heb ik de specificaties van een geautomatiseerde planningtool voor offensieve cyberoperaties vergeleken met de huidige *state of the art* in kunstmatige intelligentie. In december 2011 ga ik dat *paper* presenteren in de 29e workshop van het *UK AI Planning & Scheduling Special Interest Group*. Mijn CSIR collega's en ik, aangevuld met leden van het Universiteit van Pretoria's *Information and Computer Security Architectures* onderzoeksgroep, zijn al begonnen om tools, technieken en andere (kennis-) resources te identificeren door een systematisch analyse van het canonical procesmodel. Het is de bedoeling dat dit resulteert in een *paper* voor het 4e *international conference on Cyber Conflict* (CyCon) in juni 2012.

BESTUDEREN VAN BOEVEN

Daarna ga ik de literatuur bestuderen over hoe *bot herders* hun eigen C2 regelen, want – volgens mij – zijn ze allang op NEC Maturity Level 4. Hoogstwaarschijnlijk kunnen wij veel leren van die boeven. Werk genoeg dus aan de wetenschappelijke winkel!