CYBER OPERATIES: EEN OPERATIONS RESEARCH PERSPECTIEF

Dr. Herman Monsuur, Universitair Hoofddocent Operations Research, NLDA

Wie heeft het vroeger niet meegemaakt: Op school werden lessen aangeboden over verschillende onderwerpen. Vervolgens werd je aan een aantal tests onderworpen om het geleerde te toetsen. Hoe anders gaat het in de praktijk van alledag: Eerst krijg je een test (waar je meestal voor zakt), daarna komen de lessen aan bod die je daar uit kunt trekken.

Helaas zijn bij cyberoperaties de belangen en risico's te groot om telkens pas achteraf in staat te zijn de lessen te identificeren en ter harte te nemen. Zoals Prof. Heertje in zijn boek 'Echte economie' meldt: *'Het vermogen vooruit te zien is teloorgegaan en vervangen door verontschuldigingen vanwege wijsheid achteraf. Individuele reflectie is vervangen door publiek zelfonderzoek, nadat calamiteiten zich hebben voltrokken'*. Op de NLDA wordt de individuele verantwoordelijkheid en het nut van reflectie aangaande cyberoperaties onderkend. Zo richten de collega's van Command and Control (C2) zich bijvoorbeeld op offensieve cyberoperaties. Vanuit de Operations Research onderzoeken we een aantal kwantitatieve aspecten van cyberoperaties met behulp van (wiskundige) netwerktheorieën, speltheorie en 'stochastic-actor based' simulaties. Op deze bijdrage vanuit de Operations Research willen we nu nader ingaan.

Netwerken, ook C2 netwerken zijn ontworpen met functionaliteit als oogmerk. Maar, tegelijk zijn deze netwerken juist vanwege hun onderlinge verbindingen kwetsbaar. Om op een verantwoorde manier hiermee om te gaan, zal men proberen zoveel mogelijk dreiging (op voorhand) te elimineren, en een goede risico inschatting willen maken. Daarnaast schenkt men aandacht aan het herstellend vermogen van een netwerk nadat het doelwit is geweest van een vijandige aanval. Hierbij gaat het dus om het ontwerpen van robuuste netwerken.

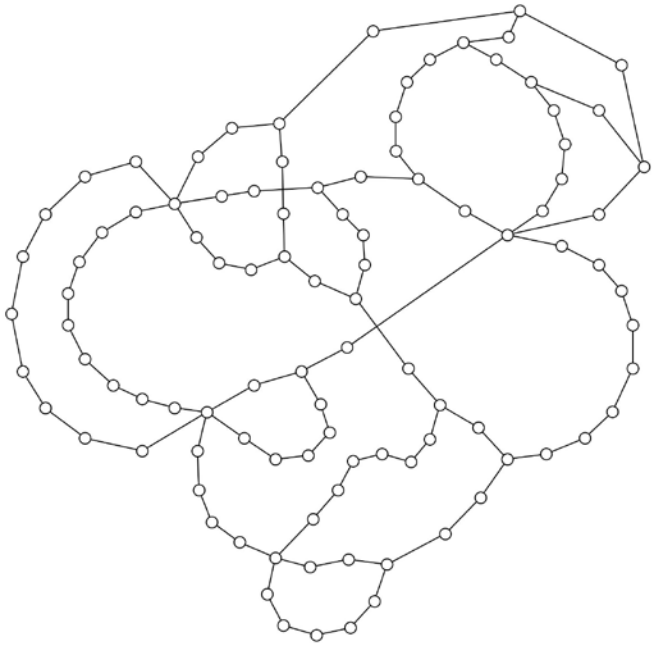
In eerder NLDA onderzoek is aannemelijk gemaakt dat de C2 netwerken, zoals TITAAN of AFSIS, geclassificeerd kunnen worden als zogenaamde schaalvrije of *preferential attachment* netwerken. Dit zijn netwerken die eruit zien als de vliegtuigroutes van bijvoorbeeld Air France/KLM: enkele knopen zoals Schiphol hebben zeer veel connecties, een groot aantal slechts één of twee. In C2 netwerken zijn deze *hubs* natuurlijk zeer kwetsbaar voor een gerichte aanval en is het resterende netwerk zonder deze hubs nauwelijks nog in staat te functioneren. Bovendien hoeft een tegenstander niet eens te weten waar de hub zich precies bevindt, want de kans is aanzienlijk dat het binnen één verbinding ligt van een willekeurig geïdentificeerde knoop. Op dit moment doen we daarom onderzoek op het gebied van netwerktheorieën om andere, meer geschikte netwerktopologieën te identificeren. Een artikel over een door ons gevonden type netwerk verschijnt binnenkort in de European Journal of Operational Research. Het basisidee hierbij is dat elke knoop in een dergelijk netwerk ten opzicht van elke ander knoop over een unieke verbinding in het netwerk beschikt, zoals in het netwerk in afbeelding 1.

Dezelfde netwerken kan men ook gebruiken om automatische zelfherstelprotocollen op te stellen na een vijandige aanval, en het netwerk zodoende robuust te maken. Hierbij maken we gebruik van *stochastic-actor based* simulaties. Deze actoren of agenten kunnen verbindingen toevoegen of verbreken. De autonome agenten zijn zo geprogrammeerd dat het uiteindelijke gerealiseerde netwerk gewenste eigenschappen bezit, bijvoorbeeld ten aanzien van de kwetsbaarheid of het gemiddeld aantal verbindingen. In november hebben we op een internationale OR conferentie deze ideeën gepresenteerd. Omdat we in staat zijn zeer veel van dergelijke netwerken te identificeren, zou dit idee ook gebruikt kunnen worden om het werkelijke netwerk dat in gebruik is te camoufleren, of om frequent te schakelen tussen verschillende netwerktopologieën om zo *traffic analysis* door een tegenstander onmogelijk te maken.

Natuurlijk kan men een netwerk trachten te beveiligen en te bewaken door bijvoorbeeld 'sensoren' te plaatsen om verdacht verkeer (virussen, wormen, etc.) te onderscheppen. Hierbij moet men zich natuurlijk wel realiseren dat niet alles kan worden bewaakt, en dat vanwege het open karakter het systeem nooit waterdicht kan en mag worden gemaakt. Omdat een tegenstander vaak in staat is om de genomen beveiligingsmaatregels te observeren, zal het risico zich verplaatsen. Een techniek die zeer behulpzaam is om optimale bescherming te realiseren tegen dergelijke intelligente, zich aanpassende tegenstanders (en gegeven allerlei randvoorwaarden als budget en inperken van onbedoelde neveneffecten) is de *speltheoretische risico analyse*. Gecombineerd met wachtrijtheorie kan dit inzichtelijk maken wat de optimale *netwerkinterdictie* strategie is en kan men een inschatting geven van het risico waarmee men moet leren leven. Deze technieken vinden hun oorsprong in bestaande methoden voor *Critical Infrastructure Protection*. Op dit moment wordt hiernaar, samen met de Universiteit Twente onderzoek naar gedaan.

SERIOUS GAMES

Tenslotte willen we, samen met andere partners ook graag aandacht schenken aan *serious games* voor cyberoperaties en 'cyber awareness'. Zonder dat er dan sprake kan zijn van calamiteiten kan men leren hoe eigen handelen een reactie van de tegenstander uitlokt. Met als ultiem doel om achteraf de vooraf geleerde lessen in de praktijk te brengen.



Afbeelding 1: Een minimaal stabiel netwerk.