CYBER SITUATIONAL AWARENESS

ANTICIPEREN IN HET DIGITALE DOMEIN

BIJDRAGE: **Peter Güldenpfennig**

IN HET MILITAIRE DOMEIN HEEFT ZICHT OP DE SITUATIE, BEGRIP VAN DE SITUATIE EN HET KUNNEN ANTICIPEREN BINNEN DEZE SITUATIE ALTIJD EEN SLEUTELROL GESPEELD BINNEN HET OPTREDEN. NIET GEK DUS DAT SITUATIONAL AWARENESS (SA) EEN BELANGRIJK ELEMENT IS IN DE C2-KETEN. IMMERS, ACCURAAT OPTREDEN KOMT VOOR EEN GROOT DEEL NEER OP HET IN KAART HEBBEN VAN JE OMGEVING EN DE DREIGINGSACTOREN.

In het cyberdomein is dat niet anders. Ook daar geldt dat "het complete plaatje" leidend is voor een goed offensief en defensief binnen dit domein en het bereiken van decision support. Voor een goed SA-beeld zijn drie elementen van belang: een volledig in kaart gebrachte computer- en netwerkinfrastructuur (network awareness), het onderkennen van dreigingen (threat awareness) en afhankelijkheden voor het optreden in cyberspace (mission awareness). Feitelijk komt dit neer op: de weerbaarheid van onze digitale infrastructuur zoals deze zich voordoet, weten welke dreigingen zich voordoen die deze infrastructuur schade kunnen toebrengen en de elementen binnen de infrastructuur die van kritiek belang zijn. Kennis hierover geeft je de mogelijkheid om je commandovoering te optimaliseren en keuzes te maken die van beslissend belang kunnen zijn in operaties.

Situational awareness versus cyber situational awareness

Hoewel situational awareness en cyber situational awareness een grote overeenkomst hebben in het in beeld brengen van een situatie om hierop te kunnen anticiperen, zijn er wel degelijk grote verschillen en daarmee ook verschillende uitdagingen.

Allereerst het domein zelf. Waar situational awareness zich vooral bezig houdt met het fysieke domein, richt cyber situational awareness zich grotendeels, met uitzondering van fysieke infrastructuren en de bijbehorende actoren , op het digitale domein. Dit betekent dat direct zicht op actoren en hun acties, of die nu bijdragen aan de digitale weerbaarheid of deze juist verminderen, op vele wijzen zijn te maskeren, wat een cyber situatie altijd gecompliceerd en uitdagend maakt.
De eerder genoemde drie elementen die zorg dragen voor een goed SA-beeld (network awareness, threat awareness, mission awareness) helpen ons om deze complexiteit te tackelen door aan elk element praktisch handelen toe te kennen:

NETWORK AWARENESS:

- Een goed gedocumenteerde en gemanagede lijst van assets en configuraties.
- Vastgestelde compliancy d.m.v. audits met een bijbehorend patch-beleid.
- Zicht op incidentmeldingen uit eigen netwerken.
- Cyberposture: de eigen houding ten opzichte van security en eigen kwetsbaarheden.
- Risicomanagement.

THREAT AWARENESS:

- Awareness over de gehele organisatie voor bestaande bedreigingen door samenwerking met partners uit het bedrijfsleven en overheid.
- Kennis van alle niveaus van karakteristieken van de verschillende dreigingsactoren; van technische indicatoren tot motivatie en drijfveren.

MISSION AWARENESS:

- Kennis van waar welke onderdelen van de IT op elk moment worden gebruikt.
- Inzicht in hoe de IT wordt gebruikt om business goals (in de vorm van bijvoorbeeld missies en oefeningen) te verwezenlijken.
- Risicoanalyse en de bijbehorende voorwaarden in het wel of niet accepteren van risico's.

Deze praktische invulling geeft handvatten, maar is slechts een begin. Dit heeft alles te maken met de complexiteit van systemen, infrastructuren en de afhankelijkheden voor deze systemen en infrastructuren. Bovendien is de automatisering van SA een samenspel tussen mens en machine, waarin de denkprocessen en interacties van de mens zich moeilijk laten modelleren.

Een volledig beeld van een snel veranderende cyberomgeving lijkt daarom ook bijna een verloren zaak. Toch worden er continu initiatieven ondernomen om het SA-beeld te verhogen, te verbeteren en te completeren. Dit laatste, een compleet SA-beeld, is uiteraard de gewenste situatie, maar helaas wel een situatie die (nog) ver van ons afstaat.

Multinational Cyber Defence Capability Development

Zowel op nationaal niveau als binnen de NAVO zijn er afgelopen jaren projecten opgestart om kennis op te bouwen over cyber situational awareness en om praktische invulling te geven aan deze kennis door middel van experimenten met demonstrators. Een voorbeeld hiervan is het NAVO-project Multinational Cyber Defence Capability Development (MN CD2), een project wat meerdere werkpakketten omvat die allemaal gericht zijn in het verhogen van cyber capabilities, waaronder ook cyber situational awareness.
Dit project heeft twee protoypes opgeleverd in samenwerking met een marktpartij.
Om de prototypes zo waarheidsgetrouw vorm te geven, is gebruik gemaakt van gegevens- en informatiebronnen zoals opgenomen in de NATO Computer Incidence Response Capability (NCIRC) Operational Deployment Capability and Exercise Reference System (NODCERS) omgeving.

Hoewel de prototypes niet volledig voldeden aan de verwachtingen en daarom ook niet hebben geleid tot een operationele oplossing, vormen deze wel een aanzet om verder te werken aan cyber situational awareness capabilities. Ook op nationaal niveau. Zo werkt het Defensie Cyber Security Center (DCSC) samen met JIVC/KIXS aan het Cyber Defence Analytics Testbed (CDAT)-experiment. Binnen CDAT worden algoritmen ontwikkeld die door training op enkele datasets informatie moet opleveren over anomalieën, de modellering van cyber space en de functionaliteiten waaraan een dergelijk systeem moet voldoen om elke gebruiker, van data-analist tot commandant, te voorzien van de juiste informatie ten behoeve van decision support. Resultaten van dit experiment moeten eind 2019 volgen.

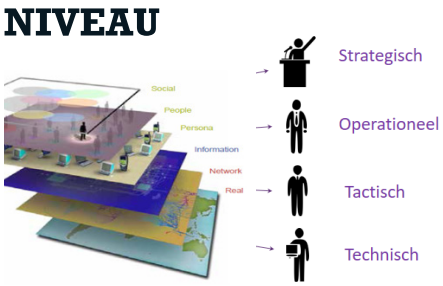
Van data naar decision support: mensen, processen en procedures

Het kwam dit artikel al eerder voorbij: de gebruiker. Want capabilities voor een goede cyber situational awareness leunen op diegene die moeten werken met de informatie die we uit het cyberbeeld halen. Of dit nu opslag of analyse van data is, het

Afbeelding 1: De opbouw van cyber situational awareness

doen van uitspraken over de informatie die we zien, of het daadwerkelijk maken van beslissingen op basis van die informatie. Met andere woorden: elke gebruiker is anders, en dat maakt het schetsen van een goed werkend cyberbeeld lastig. De digitale wereld is immers niet te vangen in een fysiek binaire wereld waarin iets wel of niet voorkomt, maar een constant veranderende omgeving die steeds weer vraagt om een specifiek handelen en dus naar specifieke kennis van een gebruiker. Dit is ook één van de redenen dat een cyber situational awareness-oplossing niet een one size fits all-oplossing kan zijn. In een militaire context: een defensief cyber emergency response team heeft andersoortige informatie en functionaliteiten nodig dan een offensieve organisatie zoals het Defensie Cyber Commando (DCC). Binnen de twee genoemde voorbeelden vallen ook weer gebruikers met andere behoeften aan informatie.

De verschillende processen en procedures in combinatie met de mensen binnen deze processen zijn randvoorwaardelijk voor het slagen van operaties en oefeningen. Combineer dit met de afhankelijkheid van technologie voor het scheppen van een zo volledig mogelijke cyber situational awareness, en je hebt een mix die lijkt te hinten naar een onneembare berg. Hoewel de verschillende behoeften binnen cyber situational awareness onderkend worden, maakt de combinatie met een steeds en snel veranderende cyber space het vinden van oplossingen hiervoor moeilijk. Dat betekent niet dat er geen oplossingen voor gevonden kunnen worden, maar wel dat goede sets aan requirements die een oplossing kunnen opleveren waar de militair in het veld echt



Afbeelding 2: Conceptuele gebruikersgroep

iets aan heeft, er één van de lange adem is. De verschillende cyber entiteiten werken in ieder geval hard in het vinden van (deel) oplossingen, in samenwerking met kenniscentra, kennisinstituten, innovatieafdelingen binnen Defensie en het bedrijfsleven.

Het besef dat stilstaan geen optie is, is doorgedrongen tot de Nederlandse krijgsmacht en dat is een goede eerste start tot iets wat hopelijk zal leiden tot een zo volledig mogelijk cyber situatie-beeld. ●

Over de auteur

Peter Güldenpfennig is innovatiemanager bij JIVC KIXS. Hier houdt hij zich met name bezig op de gebieden cyber, security en communicatie. Daarnaast is hij betrokken bij de communicatie rondom de oefening Purple NECtar.