Ministry of Defence

SBIR-pitch: Defensie-verkenningen in cyberspace

24 januari 2014

ONGERUBRICEERD/ALLEEN VOOR OFFICIEEL GEBRUIK

Inhoud

1. Aanloop naar de ontwikkeling van CNA-capaciteit
2. Verkennen van het digitale domein
3. Concrete behoefte

Adviesaanvraag regering bij AIV/CAVV

Adviesaanvraag regering (aug. 2011)

Verzoek om een advies uit te brengen over de betekenis van ontwikkelingen op cybergebied voor het Nederlandse buitenlands-, veiligheids- en defensiebeleid.

Advies AIV/CAVV (dec. 2011)

Drie typen operationele cyberactiviteiten Defensie:

- **defensieve activiteiten** (CND)
  - netwerkverdediging (passieve verdediging)
  - netwerkaanval (actieve verdediging)

- **inlichtingenactiviteiten** (CNE)
  - netwerkexploitatie

- **offensieve activiteiten** (CNA)
  - netwerkaanval

Definitie Computer Network Attack

Advies AIV/CAVV (dec. 2011)

Digitale oorlogvoering is het uitvoeren van militaire operaties die erop zijn gericht om met digitale middelen computersystemen of netwerken van een tegenstander te verstoren, misleiden, veranderen of vernietigen.

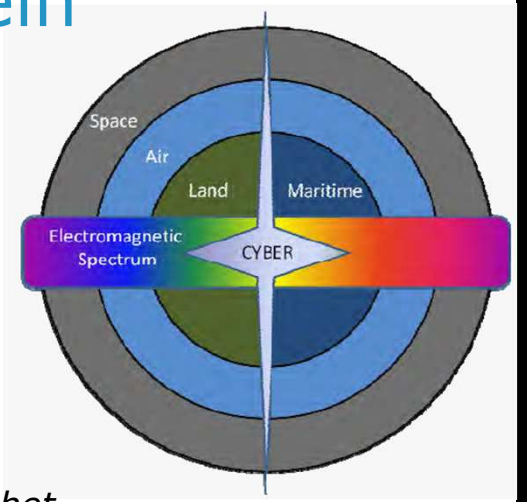
Criteria:

1. *militaire operatie met doelstelling behalen politiek/militair voordeel*
2. *berokkenen schade aan digitale infrastructuur tegenstander*
3. *door middel van inzet van digitale, niet-kinetische, middelen.*

Advies: treed op in het vijfde domein

Advies AIV/CAVV (dec. 2011)

Digitale domein beschouwen als vijfde operatiegebied dat interacteert met de andere vier dimensies voor militaire operaties. Dit betekent dat operaties in de vijfde dimensie ook kunnen fungeren als force multiplier van activiteiten in de overige dimensies.



Defensie Cyber Strategie (jun. 2012)

Het digitale domein is, naast het land, de lucht, de zee en de ruimte, het vijfde domein voor militair optreden. Dit domein en de toepassing van digitale middelen als wapen of inlichtingenmiddel zijn onmiskenbaar sterk in ontwikkeling. Digitale middelen zullen in toenemende mate integraal deel uitmaken van het militaire optreden.

Defensie Cyber Strategie (jun. 2012)

Het bezitten van een hoogwaardige inlichtingenpositie in het digitale domein is een voorwaarde voor zowel de bescherming van de eigen infrastructuur als voor de uitvoering van operaties. Defensie moet zicht hebben op de dreigingen in het digitale domein waaraan zij kan worden blootgesteld om zich daar effectief tegen te kunnen wapenen. Dit vereist inzicht in zowel de technische dreiging als de mogelijkheden en intenties van (potentiële) tegenstanders en aanvallers. De MIVD moet daarom beschikken over inlichtingencapaciteiten om deze informatie te verwerven, te analyseren en daarover tijdig te rapporteren.

Cyberaanval wordt speerpunt van nieuwe 'Defensie Cyber Strategie'

27/06/12, 11:13 – bron: ANP

© ANP. Minister van Defensie Hans Hillen

De krijgsmacht moet in de toekomst ook cyberaanvallen kunnen uitvoeren. Het wordt een van de speerpunten van de nieuwe Defensie Cyber Strategie van het ministerie van Defensie. Minister Hans Hillen maakte dat vandaag op een symposium van de Koninklijke Militaire Academie in Breda bekend.

'Als zwaardmacht moet de krijgsmacht naar mijn overtuiging ook in het digitale domein offensief kunnen optreden', stelde de bewindsman. Op dit terrein zal nauw worden samengewerkt met de militaire inlichtingendienst MIVD.

MIVD krijgt centrale rol bij digitale oorlogsvoering

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) krijgt een centrale rol als het Nederlandse leger een aanval moet uitvoeren.

Foto: ANP

Dat schrijft minister Jeanine Hennis van Defensie in een brief aan de Tweede Kamer.

Dat de inlichtingendienst zich nu ook zelf met oorlogsvoering bezig gaat houden, komt omdat voor cyberoorlog veel kennis van zaken nodig is.

Stand van zaken Defensie Cyber Strategie (aug. 2013)

Defensie zal geen afzonderlijk krijgsmachtdeel oprichten voor het optreden in het digitale domein. Bij de ontwikkeling en inzet van offensieve operationele cybercapaciteiten door de CDS zal daarom zoveel mogelijk gebruik worden gemaakt van kennis en middelen die bij de MIVD aanwezig zijn.

Actuele ontwikkelingen

"Dit [cyber] zal verder worden geïntensiveerd. In het cyberdomein gaan de ontwikkelingen immers snel. De krijgsmacht speelt daar op in. Zo wordt het Defensie Cyber Commando bij het Commando Landstrijdkrachten versneld opgericht. Enerzijds om de eigen systemen beter te beschermen en anderzijds om de benodigde offensieve capaciteit te ontwikkelen. Hierbij hoort ook de versterking van DefCERT bij IVENT evenals een versterking van de MIVD-cyberinlichtingencapaciteit."

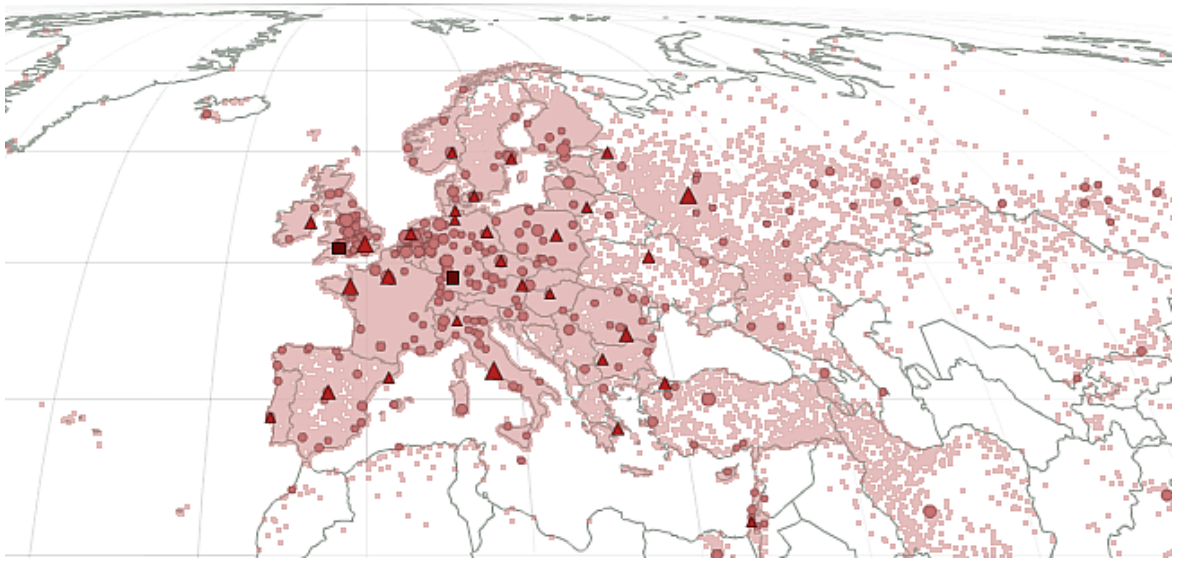
Voorbeelden van verkennen in cyberspace

1. inventariseren en in kaart brengen digitale domein (inzet IP- en poortscans, searchbots, registratiemiddelen)

2. identificeren

3. lokaliseren

4. Detecteren



Doel van verkenningen in cyberspace

Het inventariseren van de functionele aard van systemen:

- Privaat
- Publiek
- Militair
- Type server
- Industrial Control (ICS/SCADA)
- Etc.

Vastleggen technische kenmerken systemen:

- Operating system
- Applicaties
- Open en gesloten poorten
- Versie programmatuur
- Etc.

Wat we zoeken

- Programmatuur die in staat is om digitale domein in een (potentieel) missiegebied in kaart te brengen teneinde te kunnen:
  - Identificeren
  - Lokaliseren
  - Detecteren
- Modulaire opbouw
- Broncode wordt aan Defensie ter beschikking gesteld
- Bij voorkeur op basis van Linux
- Bij voorkeur geschreven in Python
- Visualisatie is van groot belang
- Zeer gebruiksvriendelijke interface
- Afgebakend zoeken en verkennen nadat het digitale domein in kaart is gebracht
- Mogelijkheden voor verkenningen met IPv6

Vervolg

- Deadline voor de call is donderdag 30 januari om 17:00 uur

Vragen?