Nota van Inlichtingen 2e tender SBIR cyber security, 24 januari 2014

Behorende bij de pitch en informatiebijeenkomst op 24 januari 2014 in Den Haag. Deze nota bevat de vragen die tijdens de bijeenkomst zijn gesteld en de antwoorden die daarop gegeven of naderhand geformuleerd zijn. Onderaan staan de 2 teksten die voorafgaand aan de pitch gepubliceerd werden bij de uitnodiging.

Vraag	**Antwoord**
1) Het is kort dag om voor de deadline nog samenwerkings-partners te vinden en afspraken te maken, hoe gaan we daarmee om?	Indien mogelijk geeft u concrete informatie over uw samenwerkingspartner, inclusief hun expertise en meerwaarde voor het project. Maakt u ook concreet hoe substantieel de samenwerking is en waar die uit bestaat. Mocht dit niet mogelijk zijn, geeft u dan minimaal aan voor welke expertise u samenwerkings-partners zoekt. De beoordelingscommissie krijgt dit als instructie mee.
2) Kost het Defensie teveel tijd om een verkenning uit te voeren op cyber security gebied, is dat het probleem?	Defensie kan u niets vertellen over de modus operandi, maar soms moet een missiegebied snel worden verkend vanwege een spoedeisend karakter, in andere gevallen is een ruimere periode voorhanden om verkenningen uit te voeren. Dat geldt ook voor verkenningen in cyberspace. N.B. Het is Defensie ook te doen om veranderingen in de tijd te kunnen volgen met behulp van bijvoorbeeld visualisaties.
3) U zoekt expertise voor de ontwikkeling van een modulair opgebouwd systeem op basis van een Linux platform, bij voorkeur geschreven in Python. Waarom richt u zich op Python?	Het Ministerie van Defensie heeft in dezen een lichte voorkeur voor Python omdat ze er goede ervaringen mee heeft. Mocht u een andere taal willen voorstellen, dan is dat in beginsel geen probleem, maar onderbouwt u svp deze keuze.
4) Naar welke systemen heeft u al gekeken in verband met kosten en toepasbaarheid?	Er is geen vergelijking gemaakt met publiekelijk beschikbare andere systemen die soortgelijke integrale functionaliteit zou kunnen bieden; de onderhavige behoefte is dermate specifiek en uniek dat deze nieuw ontwikkeld zou moeten worden. De SBIR-aanbesteding is geschikt om dit soort zaken te ontwikkelen. SBIR richt zich op alle bedrijven die in de Europese Unie zijn gevestigd om met een op maat gesneden oplossing te komen voor de vraagstukken in de oproep. Een eindgebruiker als Defensie heeft behoefte aan voorstellen voor thema 9 (win-win). Defensie zoekt een op maat gesneden voorstel dat je zou kunnen uitbreiden op termijn. Ook de komende jaren zal het onderwerp (offensieve) cyber security

	immers relevant zijn. Het gaat Defensie in dezen om verkenningen die nodig zijn om ergens een militaire operatie te kunnen uitvoeren. Vaak moeten cruciale vragen voorafgaand aan optreden al beantwoord zijn en moeten relevante delen van cyberspace in kaart zijn gebracht. Defensie zoekt innovatieve, en vooral ook praktisch toepasbare oplossingen in het licht van de effecten die we willen bereiken. Dit alles moet in uw voorstel duidelijk worden.
5) Heeft u met de eindgebruiker iedereen op het oog?	De interface moet gebruiksvriendelijk, eenvoudig en aantrekkelijk zijn omdat gebruikers het systeem intensief moeten gaan gebruiken teneinde het verder te verbeteren. De verdere ontwikkeling van de programmatuur en het systeem zijn het best geborgd bij een intensief gebruik en de daaruit voortkomende suggesties en innovaties. Het verzoek aan u is om er iets moois, aantrekkelijks van te maken zodat mensen uw product leuk vinden om ermee te werken (waardoor snelheid en efficiëntie ook een impuls krijgen). Het is belangrijk om de eindgebruiker input te laten geven en mee te laten denken. Daarvoor moet hij met al het product kunnen 'spelen' tijdens de ontwikkeling.
6) Is nagedacht over digitale camouflage?	Zie vraag 7.
7) Is het belangrijk in het voorstel mee te nemen dat verkenningen niet teruggeleid worden naar Defensie?	Nee, dat is niet belangrijk omdat Defensie daar zelf voor zorgt.
8) Bent u op zoek naar een totaal nieuw systeem of komen ook systemen in aanmerking die reeds op de markt zijn?	Defensie verschaft geen informatie over de modus operandi. Het verzoek aan u is om (bestaande) feeds, datastromen en informatie uit open of commerciële bron te combineren tot een nieuw systeem met een uitstekende visualisatie. Zie ook vraag 4.
9) Is het interessant voor Defensie om te kijken waar een digitale omgeving voor gebruikt wordt, bijvoorbeeld om een kerncentrale aan te sturen?	Ja, dat is zeker interessant en het gaat niet alleen om ICS-systemen of pc's, maar ook om bijvoorbeeld wapensystemen. Denkt u daarbij zo breed u kunt, ook in de zin van correlaties/combinaties aanbrengen: van welke ICS-systemen van een vijandelijke actor staan poorten open met besturingssysteem x versie y?
10) Gaat de interesse van Defensie ook uit naar fysieke kenmerken van aangetroffen ip-adressen of domeinen	Fysieke kenmerken zijn zeker interessant voor Defensie, zo ook of het een databases betreft of een server (en welke soort).

bijvoorbeeld?	
11) Is het feit dat er telefooncentrales in verkenningen worden aangetroffen, interessant voor Defensie?	In beginsel is ieder resultaat van verkenningen van cyberspace dat met dit systeem wordt ingewonnen interessant.
12) Defensie wil zelf gebruik kunnen maken van de broncodes, maar voor een ondernemer is dat een onaantrekkelijk vooruitzicht omdat hij daarmee zijn intellectuele eigendom verliest. Hoe ziet u dat?	Defensie stelt twee voorwaarden met betrekking tot de broncode: 1) er moeten door Defensie nieuwe modules mee geschreven kunnen worden ter uitbreiding, waarvoor de broncode dus benodigd is en 2) Defensie wil voorts zelf over de broncode beschikken om veiligheidsredenen. De broncode wordt niet met derden gedeeld.
13) Wat bedoelt u met bronnen uit open source?	Het gaat om informatie die open source beschikbaar is, Defensie zet niet de broncode op internet.
14) Waarom is de deadline zo scherp gesteld?	Voor Defensie is het geen vanzelfsprekendheid om naar buiten te treden. Het Ministerie heeft besloten het toch te doen vanwege de kansen die het SBIR-budget biedt. Vanwege allerlei obstakels die er helaas waren, is dit het vroegst mogelijke moment.
15) Is een visualisatie nodig?	Visualisatie is van groot belang. Zie ook vraag 5.
16) Heeft u een advies voor ondernemers die in willen dienen?	Dat advies luidt: think different. U kent het doel dat we willen bereiken, er zijn enkele suggesties gedaan voor middelen waarmee we dat zouden kunnen bereiken en de vereisten zijn helder: het gaat er nu om het op een innovatieve, slimme en aantrekkelijke manier bij elkaar te brengen.
17) In hoeverre zijn voorstellen gericht op telefoons ook interessant voor Defensie?	Het gaat primair om het in kaart brengen van cyberspace.

Hieronder volgen de 2 teksten die voorafgaand aan de pitch gepubliceerd werden bij de uitnodiging.

1) Den Haag, 14 januari 2014

Thema 9 Offensieve Cyber Capabilities: Verkenningen in cyberspace
Voor Defensie is het digitale domein hetzelfde als de klassieke domeinen land, de lucht, de zee en de ruimte: de krijgsmacht moet er militair in kunnen optreden. Digitale middelen zullen in toenemende mate integraal deel uitmaken van het militaire optreden.

Dat doet Defensie niet in zijn eentje. Voor de opbouw van die capaciteiten zoeken we samenwerking met de markt.

Wat we willen
Aan effectief militair optreden in het digitale domein gaat, net als bij militair optreden in de andere domeinen, een verkennende fase vooraf. Bij de ontplooiing van Nederlandse militairen in het buitenland is het daarom van belang dat voorafgaand (het relevante deel van) het lokale digitale domein in kaart is gebracht. Een goed beeld van de technische inrichting en functionele aard van systemen in het digitale domein van een (toekomstig) missiegebied is daarbij essentieel. Voorts is het van belang dat zowel de technische dreiging als de mogelijkheden en intenties van (potentiële) tegenstanders en aanvallers is geïnventariseerd. Zowel kennis van de digitale infrastructuur (systemen en netwerken) in het algemeen, alsook van relevante actoren danwel mogelijke opponenten in cyberspace in het bijzonder is daarbij noodzakelijk. Kortom, defensie zoekt naar systemen die haar kunnen helpen in de verschillende fasen van offensief cyberoptreden.

Wat we zoeken
Het doel is bovengeschetste verkennende activiteit te ondersteunen middels programmatuur die binnen strikte juridische kaders informatie binnen cyberspace vergaart. Defensie beoogt een visueel aantrekkelijke interface te laten ontwikkelen op basis van open of commerciële bronnen om digitale actoren in een (potentieel) uitzendgebied te kunnen identificeren, lokaliseren en definiëren. De functie van het systeem is in beginsel verkennend (niet-intrusief), waarbij toepassing vanzelfsprekend binnen de geldende juridische kaders plaatsvindt. Wel dient een modulaire opbouw van het systeem eventuele uitbreidingen in de sfeer van de toepassing van (intrusieve) bijzondere wettelijke bevoegdheden te kunnen faciliteren (binnen het mandaat van een missie), alsmede de mogelijkheid tot het correleren van informatie uit open bronnen met gerubriceerde informatie. De ontwikkelaar van het systeem zal de broncode aan Defensie ter beschikking stellen.

Wie we zoeken
De pitch is bedoeld voor bedrijven, organisaties en instellingen die expertise in huis hebben voor de ontwikkeling van een modulair opgebouwd systeem op basis van een Linux platform, bij voorkeur geschreven in Python, met een gebruiksvriendelijke interface waarbij afgebakend kan worden gezocht en verkend.

2) Uitwerking van uw projectidee, probleemstelling of onderzoeksvraag:
Het Ministerie van Defensie heeft in 2012 bepaald dat zij militaire operaties moet kunnen uitvoeren in het digitale domein. Daartoe moet zij beschikken over specifieke (offensieve) cybercapaciteiten. Deze capaciteiten kunnen als het ware werken als een *force multiplier* en vergroten en versterken het totale militaire vermogen van de krijgmacht en daarmee de effectiviteit.

Het gaat dus om de ontwikkeling van complexe en hoogtechnologische middelen en technieken die er specifiek op zijn gericht het totale militaire vermogen te vergroten. Offensieve cybercapaciteiten die tot doel hebben het handelen van tegenstanders te beïnvloeden of onmogelijk te maken. Capaciteiten, die kunnen worden ingezet tijdens militaire (cyber)operaties, met het primaire doel in of via het digitale domein effecten te realiseren. Zo kunnen offensieve middelen worden ingezet om een cyberaanval te

voorkomen of af te slaan en de vrijheid van handelen van het eigen militair optreden te waarborgen: "actieve verdediging". Desgewenst dragen deze effecten dus bij aan zowel een effectieve verdediging als ter ondersteuning van militaire operaties. Offensieve cybercapaciteiten worden veelal gekenmerkt door een beperkt doorzettingsvermogen, mogelijkheden en effecten zijn nog onvolledig uitgekristalliseerd en de ontwikkeling ervan is kennisintensief en daarmee kostbaar en tijdsrovend. Desalniettemin heeft Defensie zich gecommitteerd aan deze uitdaging. Daar heeft zij uw hulp, kennis en expertise hard bij nodig!

Denk bij een mogelijke oplossing aan de CIA-triad: *confidentiality*, *integrity* en *availability*. Grijp de tegenstander bijvoorbeeld aan in de logische laag2 om indirect effecten te bereiken in de sociale en/of fysieke laag; met zo min mogelijke kans op ongewenste neveneffecten en geringe kans te worden ontdekt. Kansen en mogelijkheden liggen immers in het feit dat eenieder opereert en acteert in hetzelfde digitale domein; wat voor de één geldt, geldt ook voor de ander! Het is vrijwel onmogelijk een verdediging in te richten tegen alle denkbare kwetsbaarheden en dreigingen. We beschikken helaas over "onvoldoende vingers om ieder gat te dichten". Het wegen van de risico's dus: waar voel je de pijn het ergst? Waar wordt het primaire proces, het operationele optreden het meest verstoord? Waar is de impact het grootst? Andersom is de redenatie ook van toepassing. Met welke kwetsbaarheden en dreigingen heeft een tegenstander te maken? Welke middelen heeft hij tot zijn beschikking? Hoe snel ontdekt een tegenstander een dreiging of kwetsbaarheid en, is men zich ervan bewust. Beperkt men de mogelijke dreiging om zelf in of via cyberspace te worden aangegrepen. Met andere woorden: inzicht in eigen kwetsbaarheden, in eigen middelen, eigen handelen kan leiden tot datzelfde inzicht bij tegenstanders: zij opereren immers ook in datzelfde domein.

1 Zie ter ondersteuning het artikel van kolonel P.A.L. dr. Ducheine en tweede luitenant mr. J. van Haaster in de Militaire Spectator jaargang 182, nr 9-2013 "Cyber-operaties en militair vermogen". http://jellevanhaaster.com/Artikel.pdf
2 - Beaudette, P.T. [US CYCOM]. (2013). Legal Framework for Cyber Operations. Retrieved from: cs.brown.edu/courses/cs180/lectures/Cyber_Law_for_Law_Students_120207.pdf on 21 October 2013. - United States Cyber Command [CLASSIFIED: UNCLASSIFIED]. (2013). Cyberspace: A Warfighting Domain. Retrieved form: navintpro.net/wp-content/uploads/2011/11/CYBERCOM-presentation_21OCT-NIP-EVENT.pdf on 21 October 2013.