Oproep SBIR cyber security tender III
Sluitingsdatum: 31 januari 2017, 17:00 uur

De innoverende kracht die uitgaat van verdere digitalisering in Nederland is een belangrijke stimulans voor maatschappelijke groei. Het gaat daarbij zowel om economische groei als om de mogelijkheden die digitalisering biedt aan de samenleving. Nederland zet samen met haar internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.

Cybercrime en –spionage maar ook verstoringen als gevolg van technisch of menselijk (bewust of onbewust) handelen kunnen grote schade aanbrengen en in het ergste geval maatschappelijke ontwrichting tot gevolg hebben. Daarom is het belangrijk om de weerbaarheid tegen cyberaanvallen te vergroten en vitale belangen in het cyberdomein te beschermen. Ook de aanpak van cybercriminaliteit is van belang, evenals het investeren in veilige en privacybeschermende ICT-producten en –diensten. Door te investeren in cyber security kunnen grote kosten en reputatieschade worden vermeden en innovatieve oplossingen op dit gebied mogelijk leiden tot concurrentievoordeel.

Het streven is dat de gebruiker een (groter) gerechtvaardigd vertrouwen in het gebruik van de ICT-voorzieningen ervaart. Deze 3e tender cyber security dient de weerbaarheid van onze samenleving en biedt kansen voor het ontwikkelen van expertise.

Uitdaging
De overheid daagt u als ondernemer uit om bij te dragen aan het vergroten van cyber security.

Uw voorstel moet bijdragen aan het realiseren van een of meer van de volgende hoofddoelen van de Rijksoverheid:
1. Verbeteren van de veiligheid van en het vertrouwen in de ICT-infrastructuur en -diensten.
2. Nederland voorbereiden op de veiligheidsuitdagingen (in de periode 2017-2019).
3. Stimuleren van de Nederlandse cyber security economie.
4. Realiseren van een hoogwaardig cyber security gehalte van onze vitale sectoren
5. Versterken en verbreden van kennis en innovatie op het terrein van cyber security.
6. Verbinding leggen tussen onderzoeksinitiatieven op het gebied van cyber security.

Uw voorstel moet daarbij passen binnen minstens één van de volgende 9 onderzoeksthema's uit de tweede Nationale Cybersecurity Research Agenda:
1. Management van identiteit, privacy en vertrouwen
2. Malware en kwaadaardige infrastructuren
3. Opsporing en detectie van aanvallen en monitoring
4. Forensics en incidentmanagement
5. Management van data, beleid en toegang
6. Cybercriminaliteit en de ondergrondse economie
7. Risicomanagement, economie en regulering
8. Veilige ontwerpen en technieken
9. Offensieve cybercapaciteiten

Opdrachtgever
De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van het Ministerie van Veiligheid en Justitie is opdrachtgever van de 3e tender SBIR Cyber Security. De uitvoering van de SBIR cyber security is in handen van RVO.NL. Het platform dcypher is samenwerkingspartner voor zowel de inhoudelijke en procesmatige afstemming alsook voor de matchmaking van bedrijfsleven en wetenschap. De financiering geschiedt voor 90% uit het Fonds voor interne veiligheid van de Europese Unie (ISF) en voor 10% uit eigen bijdrage van de NCTV. NWO is financier en uitvoerder van een lange termijn onderzoeksprogramma dat hierop aansluit en dezelfde onderzoeksthema's als uitgangspunt heeft.

Procedure
De ondernemers met de beste voorstellen krijgen een opdracht van de overheid om een haalbaarheidsonderzoek uit te voeren (fase 1). Fase 1 resulteert in een voorstel voor het onderzoeks- en ontwikkelingstraject (fase 2). De ondernemers met het beste voorstel voor fase 2 krijgen vervolgens een opdracht om hun project uit te voeren. Aan het eind van fase 2 moet aan de hand van een demonstratie de werking van het product worden aangetoond.

Licenties
Het is de doelstelling van de SBIR cyber security om de resultaten uit het onderzoek te delen met relevante partijen op het gebied van cyber security. Aan het eind van fase 2 demonstreren de projecten die voor fase 2 zijn gehonoreerd de resultaten van de ontwikkeling. Opdrachtgever is, in nauw overleg met dcypher, voornemens hier relevante wetenschappers, andere ondernemers en vertegenwoordigers van operationele overheidsdiensten voor uit te nodigen.

Bij deze SBIR zijn in beginsel de licentievoorwaarden van kracht die in paragrafen 4.2 en (voor fase 2) 7.2 van de SBIR-handleiding zijn opgenomen. In aanvulling hierop geldt dat in uitzonderlijke gevallen, bijvoorbeeld indien er sprake is van voorstellen die mogelijk conflicteren met de nationale veiligheid, in de contractfase individuele afspraken over intellectueel eigendom met de betreffende indiener kunnen worden gemaakt. Wanneer bij contractering (voor fase 1 of voor fase 2) geen nadere specificatie plaatsvindt van de wijze waarop opdrachtgever gebruik wil maken van de kennis zonder betaling van licentiekosten, dan vervalt dit recht van opdrachtgever.

Budget
Voor fase 1 is ca. € 940.000 beschikbaar. Het maximumbedrag per project voor fase 1 is € 30.000 incl. BTW. Voor fase 2 is minimaal € 2,4 miljoen beschikbaar. Het maximum bedrag per project voor fase 2 is € 200.000 incl. BTW. Het precieze aantal te honoreren projecten voor fase 2 is afhankelijk van de prijs van de best beoordeelde offertes voor fase 1 en fase 2. In totaal stelt de NCTV een budget beschikbaar van € 3.340.000

Beoordeling
De beoordeling vindt plaats conform de procedure zoals beschreven in de SBIR handleiding. U vindt er ook de voorwaarden en beoordelingscriteria in die voor SBIR voorstellen in het algemeen gelden.

In deze SBIR worden de volgende criteria gehanteerd. De zwaarte, uitgedrukt in punten, is eveneens vermeld.:

1) impact op de vraagstelling: 25 punten
2) ondernemerschap: 15 punten
3) innovatie: 15 punten
4) economisch perspectief: 25 punten
5) kwaliteit van het voorgestelde project: 10 punten.
6) kwaliteit van de offerte: 10 punten.

Toelichting op de criteria:

1. Impact op de vraagstelling

De commissie beoordeelt hoe groot de bijdrage is aan het oplossen van het maatschappelijk vraagstuk waar de uitdaging (zie pagina 1) zich op richt, waarbij een of meer van de onderstaande doelen in acht worden genomen:

- *Verbeteren van de veiligheid van en het vertrouwen in de ICT-infrastructuur en -diensten.* Hierbij kan (niet uitsluitend) gedacht worden aan een veilige ICT-infrastructuur met kenmerken als:
    - continuïteit van de netwerk- en informatiestructuur, zowel vast als mobiel
    - weerbaarheid/vitaliteit van de netwerk- en informatie infrastructuur, zowel in Nederland als in internationaal verband (door samenwerking met de internationale partners).
    - informatie aan de eindgebruiker in relatie tot handelingsperspectief. Dit om het bewustzijn van een veilig en betrouwbaar gebruik van ICT en telecom op een hoog peil te houden.
    - intrinsieke veiligheid van de hard- en software die wordt toegepast, zowel ten behoeve van de netwerken (infrastructuur) als de diensten.

  De scope kan gericht zijn op zowel preventie als respons.
- *Nederland voorbereiden op de veiligheidsuitdagingen (in de periode 2017-2019)*
  Het betreft hier dreigingen die zich snel ontwikkelen en waarvan de aanpak kennisintensief is. Aangezien de digitalisering van onze samenleving steeds verder toeneemt, is het van wezenlijk belang dat cyberdreigingen zowel op de korte als op de lange termijn geadresseerd worden. Het gaat hier dan om onder andere het ontwikkelen van capaciteiten als 'situational awareness in cyberspace' en de mogelijkheid de attributie van cyberaanvallen vast te stellen, maar ook om ontwikkelingen als 'security by design' en het tijdig kunnen beschikken over kwalitatief goede dreigings- en risicoanalyses.
- *Stimuleren van de Nederlandse cyber security economie*
  Het Nederlandse bedrijfsleven kent in internationaal perspectief een vooraanstaande positie op het gebied van de bestrijding van cyberthreats. Het streefbeeld is hier kennis te verdiepen en te verbreden om deze positie te behouden, door vooral in te zetten op innovatiemogelijkheden.
- *Realiseren van een hoogwaardig cyber security gehalte van onze vitale sectoren*
  Het borgen van de continuïteit van vitale processen en diensten, waaronder industriële automatisering en op afstand bediende aansturing van deze netwerken, blijft de hoogste prioriteit hebben
- *Versterken en verbreden van kennis en innovatie op het terrein van cyber security*
  Relevant is aan te sluiten bij, of gebruik te maken van, kennis en inzichten van internationale toonaangevende kennisinstellingen. Door de nauwe samenwerking van wetenschap en markt wordt zowel de innovatie bevorderd als meer inzet gepleegd om meer studenten en kennis aan deze topsector te kunnen binden. Bij de onderzoekstender zal multidisciplinair onderzoek vooral worden bevorderd.
- *Verbinding leggen tussen onderzoeksinitiatieven op het gebied van cyber security*

Wanneer er verbindingen tussen deze onderzoeksinitiatieven, al dan niet internationaal, gelegd kunnen worden kunnen onderzoeksinitiatieven elkaar versterken en kunnen schaarse middelen efficiënter gealloceerd of gebundeld worden.

De commissie kijkt nadrukkelijk naar de manier waarop invulling wordt gegeven aan één of meerdere van de op pagina 1 genoemde onderzoeksthema's uit de NCSRA.

De commissie weegt de impact van het project af tegen de kosten van het project.

2. Ondernemerschap

De commissie beoordeelt in welke mate de aanbieder de juiste partij is om zowel de ontwikkeling als de marktintroductie van de innovatie succesvol te laten verlopen. Aspecten die daarbij een rol kunnen spelen zijn ambitie, kennis, kunde en ervaring. De commissie kijkt hierbij ook naar de projectpartners. Een voorstel scoort beter naarmate

a) De verbinding met onderzoeksinitiatieven op het gebied van cyber security sterker is (bijvoorbeeld door de betrokkenheid van consortiumpartners die al eerder actief zijn geweest in vergelijkbare onderzoekstrajecten).
b) Relevante wetenschappelijke onderwijs-/kennisinstellingen betrokken zijn bij de totstandkoming van de innovatie.
c) Operationele eindgebruikers of cruciale intermediairs als internetproviders betrokken zijn bij de totstandkoming van de innovatie.
d) Er een klankbordgroep/stuurgroep/adviesraad wordt ingesteld waarin diverse vertegenwoordigers zitting nemen:
    - Een potentiële afnemer
    - Een kennisinstelling
    - Iemand met kennis van marketing/sales/productontwikkeling
    - Een organisatie die bekend is met SBIR trajecten

3. Innovatie

De commissie beoordeelt de mate van innovativiteit van het te ontwikkelen product. Aspecten die daarbij een rol spelen zijn originaliteit en inventiviteit. Een doorbraak of grote vernieuwing op één of meerdere van de thema's scoort hoger dan een marginale verbetering. Ook wezenlijk nieuwe toepassingen van een bestaand product of het verbeteren (bijvoorbeeld goedkoper, efficiënter of laagdrempeliger maken) van een bewezen techniek/product worden aangemerkt als innovatie.

4. Economisch perspectief

De commissie beoordeelt de kans dat het product succesvol op de markt kan worden gebracht. Aspecten die daarbij een rol kunnen spelen zijn: de waarde van het intellectueel eigendom, het probleem waar de innovatie op inspeelt, de waarde die het product oplevert voor klanten, de bereidwilligheid om hiervoor te betalen en de toegang tot de markt. In dit kader worden de uitkomsten van een eigen marktonderzoek (interviews, raadplegen van bronnen) en de actieve betrokkenheid van eindgebruikers als belangrijke elementen gezien. De commissie kijkt ook naar de uitwerking van het verdienmodel.

5. Kwaliteit van het project

De commissie beoordeelt hoeveel vertrouwen zij heeft, op basis van de offerte, in de succesvolle realisatie van de beoogde resultaten. De commissie beoordeelt daarbij:

- De kwaliteit van het project. Leidt het project zoals voorgesteld tot de beoogde resultaten? Hierbij zal onder andere worden gekeken naar de opzet van het projectplan en de gekozen methoden en technieken om tot een resultaat te komen.
- De commissie kijkt ook naar de projectrisico's die door de indieners worden onderkend en de mogelijke oplossingen die hiervoor worden aangedragen.
- De projectplanning. Is de projectplanning voldoende uitgewerkt (deeldeliverables) en wordt hierin ook rekening gehouden met mogelijke projectrisico's?

6. Kwaliteit van de offerte

Uit de offerte moet duidelijk blijken wat het doel is, welke onderzoeksvragen er beantwoord moeten worden, waarom bestaande oplossingen niet afdoende zijn en waarom het voorgestelde onderzoek dat wel zal zijn. De commissie beoordeelt hoeveel vertrouwen zij heeft, op basis van de offerte, in de succesvolle realisatie van de beoogde resultaten. De commissie beoordeelt daarbij:

- De kwaliteit van de offerte. Is de offerte voldoende concreet? Is duidelijk wat de resultaten zullen zijn? Is het voorstel helder geschreven? Is het voorstel to the point en voldoet het aan de richtlijnen uit de voorgeschreven formats? Is duidelijk wat de aanbieder van plan is? Geeft de offerte voldoende houvast voor een opdracht?
- De kwaliteit van de management summary. De management summary is bondig, maar voldoende informatie om te begrijpen wat het doel van het onderzoek is en waarom de aanbieder de juiste partij is om dit onderzoek uit te voeren.

Informatiebijeenkomst

Tijdens de Seaside Matchmaking Cyber security op 14 oktober 2016 in het Zuiderstrandtheater te Den Haag is uitleg gegeven over de inhoud en de procedures van deze specifieke SBIR-uitdaging. De presentatie en Nota van Inlichtingen zijn te vinden op de website van RVO.nl. Houdt deze website ook in de gaten voor de aankondiging van volgende informatiebijeenkomsten.

Tijdpad

Sluiting tender: 31 januari 2017, 17.00 uur
Bekendmaking uitslag fase 1: 1 april 2017
Opdrachtverstrekking fase 1: 15 april 2017
Opleveren eindrapport fase 1: 15 oktober 2017
Deadline offerte fase 2: 15 november 2017, 17.00 uur
Presentatie aan commissie: december 2017
Bekendmaking uitslag fase 2: januari 2018
Opdrachtverstrekking fase 2: 15 januari 2018
Deadline eindrapport fase 2: 15 juli 2019

Balancing Security and Mobility

Deze SBIR tender cybersecurity wordt medegefinancierd door het Fonds voor interne veiligheid van de Europese Unie