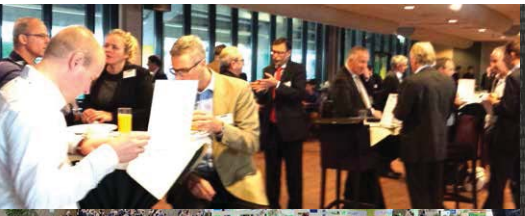
Magazine van het ICT-onderzoek Platform Nederland (IPN)
Jaargang 10 / nummer 4 / december 2013

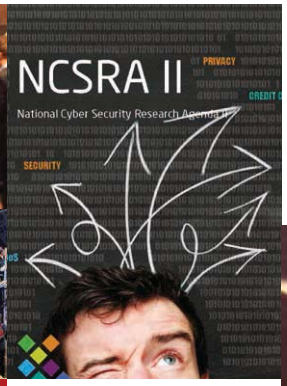
ICT-onderzoek

10

Tweede Nationale Cyber Security Research Agenda ziet het licht

Terugblik op ICT.OPEN
Winnaar Spinozapremie Piek Vossen
Marieke Huisman wint Nederlandse ICT-onderzoeksprijs





Editorial

De afgelopen maanden vielen diverse ICT-onderzoekers in de prijzen. Piek Vossen ontving in september de Spinozapremie, de hoogste Nederlandse onderscheiding in de wetenschap. Die ging voor het eerst naar een onderzoeker uit ons vakgebied. Marieke Huisman kreeg in oktober de eveneens zeer prestigieuze Nederlandse ICT-onderzoeksprijs. Tot slot mocht Yiğit Mahsereci in november de ICT.OPEN Poster Award in ontvangst nemen. Naast interviews met de drie prijswinnaars spraken we voor dit nummer met een auteur en een reviewer van de tweede Nationale Cyber Security Research Agenda. Ook besteden we aandacht aan de eerste editie van 'ICT with Industry', een event waarin onderzoekers werken aan uitdagende problemen uit de praktijk.
Heb je opmerkingen of suggesties voor nieuwe artikelen, mail dan naar ipn@nwo.nl.
For our international readers we have included summaries in English. Comments and suggestions for future articles, please email them to: ipn@nwo.nl.

I/O ICT-Onderzoek is een uitgave van het ICT-Onderzoek Platform Nederland (IPN) en wordt vier maal per jaar gratis toegezonden aan ICT-onderzoekers en relaties van het IPN.

IPN bestaat uit de informaticaonderzoeksscholen ASCI, IPA en SIKS, de onderzoeksinstituten CWI en NIRICT en de platforms SAFE en ProRISC. IPN wordt ondersteund door NWO Exacte Wetenschappen en de Technologiestichting STW. IPN is een landelijk overlegorgaan met als doel de ICT in Nederland als wetenschappelijke discipline een sterkere positie te geven. IPN wil de Nederlandse ICT-inspanningen coördineren en daarbij fungeren als hét aanspreekpunt voor ICT-onderzoek richting beleidsmakers, politiek, bedrijfsleven en andere maatschappelijke groeperingen.

Redactie Laura Jansen, Margriet Jansz, Marion van Oeveren, Astrid Zuurbier
Coördinatie Marion van Oeveren
Eindredactie Daphne Riksen

Aan dit nummer werkten mee
Jan Piet Barthel, Leendert van der Ent, Edith van Gameren, Paul Klint, Sonja Knols, Bennie Mols, David Redeker, Daphne Riksen

Redactieadres Secretariaat IPN, p/a Chemische & Exacte Wetenschappen Postbus 93460, 2509 AL Den Haag Telefoon 070 349 42 15 E-mail ipn@nwo.nl Web *www.ictonderzoek.net*

Ontwerp en opmaak Katja Hilberg Ontwerpers
Fotografie Peter van Beek, Sjoerd van der Hucht, Job Jansweijer, Lorentz Center, Shutterstock, Marijn de Wijs, Peter Lowie
Drukwerk Veenman+

IPN ICT-Onderzoek Platform Nederland

NWO
Nederlandse Organisatie voor Wetenschappelijk Onderzoek
Cluster Chemische en Exacte Wetenschappen

Digitale spionage binnen overheid, burgermaatschappij en industrie domineert het nieuws. Cybercriminelen zorgen voor een onophoudelijke stroom DDoS-aanvallen, virussen, malware, botnets, skimming, phishing en wat al niet meer, waarmee ze flinke economische schade toebrengen. Dit alles maakt de tweede Nationale Cyber Security Research Agenda uiterst actueel. Hij biedt een brede benadering van de problematiek. Kernpunt is dat het bedrijfsleven aanhaakt bij de uitvoering. Wetenschap en bedrijven zoeken naar de match. *Door Leendert van der Ent*

Tweede Nationale Cyber Security Research Agenda
Multidisciplinair en open voor samenwerking

Herbert Bos is hoogleraar Systems and Network Security aan de VU en bestuurslid van het ICT-Innovatieplatform Security & Privacy Veilig Verbonden

'De eerste agenda uit 2011 kreeg veel waardering', constateert prof.dr.ir. Herbert Bos. 'Hij werd bijvoorbeeld internationaal opgepikt, getuige de inhoud van het recent gepubliceerde *Red Book – A Roadmap for Systems Security Research*, waarin veel van de agenda terugkomt. Een kritiekpuntje was het ontbreken van offensieve cyber security. Het onderzoeksterrein dat zich bezighoudt met het "terughacken" van criminelen staat nu in onze update.'
Bos, hoogleraar Systems and Network Security aan de VU en bestuurslid van het ICT-Innovatieplatform Security & Privacy Veilig Verbonden (IIP-VV), is samen met prof.dr. Sandro Etalle (TU/e), ir. Frank Fransen (TNO) en dr.ir. Erik Poll (RU) schrijver van de agenda (zie kader). Bos: 'De thema's blijven verder grotendeels dezelfde. We hebben de input vanuit de eerste onderzoekstender van zomer 2012 en vanuit een veldraadpleging erin verwerkt. In die call voor EUR 6,3 miljoen, uitgeschreven door NWO en Agentschap NL, zaten lange- en kortetermijn-projecten, die nu volop in uitvoering zijn.' >>

'Ook "terughacken" van criminelen staat nu in de onderzoeksagenda'

Brede benadering

De projecten zijn zeer divers. Die brede scope, ook in de nieuwe agenda, is bewust aangehouden. Bos: 'Alles over cyber security kan erin. Wij hebben niet geprioriteerd, want het is niet objectief vast te stellen wat de belangrijkste problemen zijn. Het kan zijn dat financiers zoals bedrijven en ministeries later wel een prioriteit gaan aanbrengen. Inschrijvingen van overheden en bedrijven op de calls zullen ook deels bepalen welke kant het opgaat.'
Ook is onderzoek opgenomen vanuit de gammawetenschappen, economie en recht. Bos licht toe: 'Een criminologisch onderzoeksproject probeert bijvoorbeeld hackers te profileren: wat voor opleiding hebben ze, hoe komen ze in cybercrime terecht? Soms is het bizar dat iets tot nu toe nog niet is uitgezocht, zoals hoe je de schade van een cyberaanval vaststelt. Weer andere aspecten zijn de zin van softwarecertificering en de (on)veiligheid van het 'Bring your own device'-model, waarbij het privé en zakelijk gebruik van apparaten door elkaar lopen.'

'We juichen het initiatief en de manier waarop de agenda is opgesteld toe: met aandacht voor zowel de belangen van onderzoeksinstellingen als de BV Nederland'

Dr. Wim Hafkamp was blij verrast met de gamma-onderwerpen. Hij is hoofd Information Security & Risk Management bij Rabobank, bestuurslid van IIP-VV, reviewer van de NCRSA-II en voorzitter van het Financial Institutions Information Sharing and Analysis Center (FI-ISAC). 'Wij zijn blij met de stappen die de NCSRA-I en II zetten. De agenda gaat niet apart in op betalingsverkeer, maar noemt wel aspecten die kunnen bijdragen aan een nog veiliger betalingsverkeer. Dat geldt bijvoorbeeld voor het in kaart brengen en analyseren van Botnets, de ontwikkeling van bancaire virussen – en hopelijk het vernietigen ervan. Technologie en sociaal-psychologische aspecten zijn allebei belangrijk. Die laatste bleven tot nu toe onderbelicht. Alle belanghebbenden kunnen veel leren van de resultaten die daaruit zullen komen.'

Wim Hafkamp is hoofd Information Security & Risk Management bij Rabobank, bestuurslid van het ICT-Innovatieplatform Security & Privacy Veilig Verbonden en voorzitter van het Financial Institutions Information Sharing and Analysis Center

De Nationale Cyber Security Research Agenda I en II
Bij het begin van de Alert-Online campagne, eind oktober, lanceerde minister Opstelten de Nationale Cyber Security Strategie (NCSS2). Eén doelstelling van de strategie is dat 'Nederland beschikt over voldoende cyber security kennis en kunde en investeert in ICT-innovatie om onze cyber security doelstellingen te behalen'. Dat is precies waarin de NCSRA-II wil voorzien. Het ICT-Innovatieplatform Security & Privacy Veilig Verbonden (IIP-VV), dat onderzoekers uit industrie en kennisinstellingen, gebruikers en overheidsvertegenwoordigers verenigt, heeft de agenda samengesteld. Dat gebeurde op initiatief van de ministeries van Defensie, Veiligheid & Justitie, Economische Zaken, Binnenlandse Zaken & Koninkrijksrelaties en NWO (EW en STW). Deze ministeries en NWO-onderdelen zijn tevens financier van een tweede onderzoekstender van EUR 6,4 miljoen, met de NCSRA-II als vertrekpunt. Inmiddels hebben zich bij dit rijtje financiers nog de ministeries van Financiën en Infrastructuur & Milieu gevoegd, evenals NWO Maatschappij- en Gedragswetenschappen. NWO financiert het lange termijn wetenschappelijk onderzoek in publiek-private samenwerkingsverbanden met EUR 3,5 miljoen. Voor de korte termijn R&D projecten hebben de genoemde ministeries EUR 2,9 miljoen uitgetrokken. Het thema cyber security is ook onderdeel van de ICT Roadmap.

Onderzoeksthema's en toepassingsgebieden van de Nationale Cyber Security Research Agenda II

De agenda richt zich op negen onderzoeksthema's:
1 Identiteits-, privacy- en trust-management
2 Malware en kwaadaardige infrastructuren
3 Aanvalsdetectie en -preventie en monitoring
4 Forensische aspecten en incident-management
5 Data, beleid en toegangsmanagement
6 Cybercrime en de ondergrondse economie
7 Risicomanagement, economie en regulering
8 Veilig ontwerpen en ontwikkelen
9 Offensieve cyber-capaciteiten

Het addendum verduidelijkt de context en scope van de agenda met praktische en concrete voorbeelden van (mogelijke) onderzoeksrichtingen en projecten.
Meer informatie: *http://www.nwo.nl/onderzoek-en-resultaten/programmas/cyber+security* en *http://www.agentschapnl.nl/subsidies-regelingen/sbir/veiligheid/sbir-cyber-security-II*

Hardcore ICT-onderzoek bevat de agenda natuurlijk ook ruimschoots.
Eén aspect zijn de achterdeurtjes in netwerk-hardware. Zulke 'backdoors' zijn soms verplicht om bij een defect data bereikbaar te houden, maar zitten vaak heel goed verborgen waardoor je geen idee hebt dat er allerlei extra functionaliteit in je apparaat zit. Waar leiden die achterdeuren in de veelal Chinese en Amerikaanse apparatuur eigenlijk heen? Zijn ze ingesteld om informatie weg te sluizen en bieden ze wellicht de mogelijkheid om hele netwerken plat te gooien? Bos: 'De antwoorden zijn maar moeizaam uit de "black box" te halen. Behalve in de firmware kan er ook extra functionaliteit in de gebruikte IC's zijn meegebakken. De hele reverse engineering op dit gebied staat nog in de kinderschoenen.'

Samenwerking

Bij overheden staat cyber security inmiddels duidelijk op de agenda. Bos: 'Defensie maakt ondanks alle bezuinigingen geld vrij voor de Cyber Taskforce. Ook minister Opstelten heeft het onderwerp duidelijk op de agenda gezet.'
Het topsectorenbeleid wil bedrijven motiveren om flink te participeren in onderzoek. 'Cash zul je als onderzoeker niet gemakkelijk krijgen', weet Bos. 'Bij commitment en bijdragen in natura ligt dat vaak anders, zoals de inzet van bedrijfsonderzoekers en het gebruik van apparatuur, software en data.'
De belangstelling voor praktijkgericht kortetermijnonderzoek is groter dan voor fundamenteler langetermijnonderzoek. Hafkamp: 'De NCSRA-II is een research-agenda, daarop hoort ook fundamenteel onderzoek. Op de lange termijn kan dat voor banken vruchten afwerpen. Maar het leidt niet tot kant-en-klare beveiligingsoplossingen. Banken zullen eerder instappen als ze snel een direct belang kunnen veiligstellen. We zullen meedoen aan het komende matchmaking event, waarbij we benieuwd zijn naar de mogelijkheden. Voor onderzoekers naar veiligheidsoplossingen staat veiligheid voorop, maar andere aspecten zijn evenzeer belangrijk. Bedrijven zoeken de juiste balans tussen veiligheid, gebruiksgemak en beheerlast.'

Belangstelling of deelname?

In het algemeen neemt het belang van ICT bij banken verder toe, constateert Hafkamp. '*Straight-to-processing* groeit, het menselijk handelen verdwijnt uit steeds meer processen. Neem bijvoorbeeld de aanvraag van een nieuwe bankpas. Dat is goed te "STP-en". Het betekent wel dat monitoring van deze processen en goede authenticatie van de klant steeds belangrijker worden. De research-agenda kan daar antwoorden op formuleren.'
Banken volgen de wetenschappelijke ontwikkelingen op de voet, maar toch kreeg de eerste tender geen participatie vanuit de bankensector. De wetenschap zal rond deelname ook nog rekening moeten houden met bedrijfsprocedures, weet Bos. 'Het lukte niet om tijdig van hogerhand toestemming voor deelname te krijgen. We hopen dat ze bij de nieuwe tender eind 2013 wel instappen.'
Bos ziet bijvoorbeeld secure design en intrusion detection als een interessante onderwerpen voor samenwerking met de bankensector en de gezondheidszorg. 'Veel cybercriminelen richten hun pijlen op de bankensector. Volgens mij kan het voor banken vruchtbaar zijn om security-aspecten gezamenlijk met de onderzoekswereld aan te pakken. Alleen al omdat ze hooggekwalificeerd personeel nodig hebben – daaraan is op dit gebied een schreeuwend tekort. Via de doorstroming van aio's is een goede match mogelijk. Bovendien is het sowieso nuttig elkaar te leren kennen en de weg te weten in elkaars wereld.'

Wapenwedloop

Hafkamp bevestigt het beeld van een soort dagelijkse wapenwedloop tussen cybercriminelen en banken, maar ziet dat de banken vooruitgang boeken in deze wedloop: 'We moeten alert zijn en blijven. Het gaat de goede kant op.
De Nederlandse Vereniging van Banken (NVB) publiceert halfjaarlijks fraude-cijfers. De schade door cybercriminelen aan internetbankieren is sterk gedaald, van EUR 34,8 miljoen over heel 2012 tot EUR 4,2 miljoen de eerste helft 2013.' Dat is deels dankzij ICT-gerelateerde maatregelen, maar vooral dankzij publieksvoorlichting. 'De goede samenwerking tussen banken onderling en

>>

overheidspartijen helpt', voegt Hafkamp toe, 'bijvoorbeeld met de Nationale Politie via de Electronic Crime Taskforce.' Onlangs was er een doorbraak, waarbij de hoofdverantwoordelijken achter bancaire malware konden worden opgepakt. Hafkamp: 'Dit ondersteunt het idee achter de NCSRA-II: bestrijding van cybercrime vraagt om samenwerking en een multidisciplinaire aanpak van ICT met andere specialisaties. We juichen het initiatief en de manier waarop de agenda is opgesteld toe: met aandacht voor zowel de belangen van onderzoeksinstellingen als de BV Nederland.'

De overhandiging van de Nationale Cyber Security Research Agenda (NCSRA) II aan Mark Dierikx, Directeur-Generaal voor Energie, Telecom en Mededinging door Dick Brandt, voorzitter van het IIP-VV (foto: Sjoerd van der Hucht)

Overhandiging en debat NCSRA-II

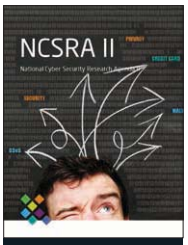
Op 4 november vond onder de noemer 'Cyber Security Onderzoek en Beleid' in Nieuwspoort de uitreiking plaats van de tweede Nationale Cyber Security Research Agenda (NCSRA-II). Dick Brandt, voorzitter van IIP-VV bood onder grote publieke belangstelling de agenda aan Mark Dierikx aan, Directeur-Generaal voor Energie, Telecom en Mededinging. In zijn dankwoord noemde Dierikx, mede namens NWO, de agenda een goede basis voor subsidierondes voor kortetermijn-R&D – waar marktpartijen het initiatief nemen – en voor langetermijnonderzoek, waarin de wetenschap het voortouw neemt. Er volgde een levendig debat onder leiding van professor Bart Jacobs over het belang van wetenschappelijk onderzoek voor cyber security. De deelnemende politici en bestuurders uit bedrijfsleven, wetenschap en onderzoeksfinanciering onderschrijven dat investeren in wetenschappelijk onderzoek cruciaal is voor een veilig digitaal Nederland. Ook vinden ze dat cyber security onderdeel moet uitmaken van topoverleg binnen bedrijven en overheden. Bovendien menen ze dat investeren in cyber security ons land enorme economische kansen biedt.

With cybercrime and cyber espionage all over newspaper's front pages, the second National Cyber Security Research Agenda II comes at the right time. It offers a broad approach. A crucial point now is for the market to embrace research project proposals and to start collaboration between companies and knowledge institutions. For short term practical projects this will be much easier to attain than for long term fundamental developments, although the market admits it also has an interest there. Practical barriers around IP, corporate processes and the public nature of research results can probably be overcome, provided that partners are really committed to cooperation, according to Professor Herbert Bos of VU University Amsterdam and cyber safety specialist Wim Hafkamp (Rabobank).

Spelregels afspreken

Voor een deel zullen de spelregels voor samenwerking tussen (bank)bedrijven en onderzoekers nog moeten worden ontworpen. Wetenschappelijk onderzoek kenmerkt zich door openbaarheid van resultaten: publicaties zijn het product bij uitstek en software-ontwikkeling is normaal gesproken open source. Intellectueel eigendom (IP) ligt dus gevoelig, maar verschillende sectoren zoals de chemie en de biotechnologie hebben daarvoor al oplossingen ontwikkeld. Bij cybercrime liggen de zaken nog iets lastiger. Bedrijven willen liever niet dat hun data, analyses van kwetsbaarheden of de inhoud van oplossingen op straat komen te liggen. Hafkamp: 'Er is een spanningsveld tussen de noodzaak om bruikbare operationele gegevens ter beschikking te stellen voor onderzoek en het feit dat privacygevoelige informatie niet openbaar mag worden.'
Bos: 'We moeten als wetenschap rekening houden met gevoeligheden. Dat kan best, via de benadering van *responsible disclosure*. Zelf heb ik een ERC-grant over reverse engineering van malware, waarbij een ethische commissie meekijkt. Als je goed nadenkt hoe je publiceert, kun je zowel aan de belangen van bedrijven als die van de wetenschap recht doen.' Hafkamp: 'Een andere mogelijkheid is contractonderzoek. Ik ben het met Herbert eens dat daar wel uit is te komen. Hetzelfde geldt misschien ook voor het tijdsaspect. Voor een ad hoc-probleem kun je niet vier jaar op de oplossing van een aio wachten, maar wellicht zijn er ook mogelijkheden voor het gebruik van tussentijdse resultaten. Als je bereid bent tot afspraken is er veel mogelijk.' I/O

Meer informatie:
Fraudecijfers bij internetbankieren: *www.nvb.nl*
De NCSRA-II (inclusief addendum): *www.iipvv.nl*



De National Cyber Security Research Agenda II

In september won The Amsterdam Institute for Advanced Metropolitan Solutions (AMS) een wedstrijd van de gemeente Amsterdam voor een nieuw kennisinstituut voor toegepaste technologie. AMS is een samenwerkingsverband van TU Delft, Wageningen UR en MIT en diverse bedrijven en maatschappelijke organisaties. Drs. Chris Karman coördineerde het voorstel namens Wageningen UR. *Door Daphne Riksen*

Sensing the city, designing the city, integrating the city

Waarom wil Amsterdam een technologisch kennisinstituut?

'Amsterdam is op zoek naar een nieuwe impuls voor de stad. Zo'n kennisinstituut geeft dynamiek, trekt talent aan en leidt tot economische spin-off. De gemeente wil bovendien de stad gebruiken als experimenteerruimte, waar nieuwe oplossingen kunnen worden uitgeprobeerd. Binnen die kaders hebben we – in eerste instantie met de TU Delft, later met MIT erbij – vanuit onze eigen ambities een voorstel geschreven en daarin onze ideeën uitgewerkt. AMS richt zich op grootstedelijke problematiek, denk aan onderwerpen als water, energie, afval en voedsel. We willen zowel onderwijs geven als onderzoek doen. En Wageningen UR wil laten zien dat onze kennis en oplossingen voor het landelijk gebied ook relevant zijn voor de steden van de toekomst.'

Hoe zien de plannen eruit op het gebied van onderwijs?

'We gaan een gezamenlijke tweejarige master Metropolitan Solutions ontwikkelen in twee vormen. De traditionele vorm wordt een combinatie van bestaande en nieuwe opleidingen en speelt zich deels af in Wageningen en Delft. Een belangrijk deel hiervan vindt plaats in Amsterdam, gekoppeld aan de living labs die we daar gaan opzetten. MIT zal gastcolleges verzorgen. Daarnaast komen we in een latere fase met een moderne variant in de vorm van Massive Open Online Courses (MOOC's). Daardoor kunnen studenten uit de hele wereld online colleges volgen en vervolgens onze *summer school* bijwonen. Degenen die daar succesvol doorheen komen, doen in Nederland het tweede jaar van de master. We gaan op termijn uit van 200 tot 250 studenten. Instromen kunnen mensen die breed geïnteresseerd zijn in grootstedelijke problematiek en een bachelor hebben in *life sciences*, bouwkunde, sociale wetenschappen en ICT of met een bestuurlijke achtergrond.'

En de onderzoekspoot, hoe ziet die eruit?
'In AMS vindt straks zowel wetenschappelijk als toegepast onderzoek plaats binnen een portfolio van projecten en programma's. Dat doen we samen met overheden en bedrijven in het *living lab* in Amsterdam. Maar ook in andere steden willen we nieuwe concepten en ideeën uittesten. Zoals Boston, een stad die zich al aan ons initiatief heeft verbonden. Over tien jaar hopen we zo'n 125 onderzoekers aan het werk te hebben.
De infrastructuur onder het onderwijs en onderzoek is de derde pijler van AMS. In dat zogenaamde *value* platform zal ICT een belangrijke rol spelen. Als je de stad gaat gebruiken als experimenteerruimte, gebruik je een grote hoeveelheid sensoren om de energie-, afval-, grondstof-, verkeer- of mensenstromen te meten. Al die data, ook afkomstig van andere steden, worden via het mobiele datanetwerk bij elkaar gebracht en via ons *value* platform ontsloten.
Overigens doen we dat niet alleen voor onderwijs en onderzoek, maar ook voor bedrijven die daar gebruik van wil maken. Het belang van data-analyse en -verwerking zal alleen maar groter worden naarmate AMS zich verder ontwikkelt.'

Ziet u daarnaast nog een andere rol weggelegd voor ICT?

'Ons motto is "sensing the city, designing the city, integrating the city". Ik zie voor ICT vooral een grote rol weggelegd in het eerste, maar eigenlijk zit ICT overal in. Denk maar aan het gebruik van MOOC's in de masteropleiding. ICT-innovatie zal ook zeker terugkomen in de oplossingen die je in de stad gaat uittesten en aanbrengen. En ook in het value platform zien we nog veel ICT-uitdagingen.'

Wanneer gaat AMS echt van start?

'We zijn nu in onderhandeling met de gemeente Amsterdam over de verdere vormgeving van AMS, zoals hoe en waar we het instituut gaan vestigen. Medio 2014 willen we formeel van start gaan, maar er zitten al projecten in de pijplijn die we eerder aan Amsterdam kunnen koppelen en ook het onderwijs kan op onderdelen snel beginnen.' I/O

Rectificatie

In het vorige nummer van I/O Magazine kwam op deze plaats Marc van den Homberg (TNO) aan het woord. Bij het door hem genoemde project in Mali op het gebied van mobiele spraaktechnologieën voor arme boeren werd ten onrechte de indruk gewekt dat dit een TNO-project is. VOICES is echter een door EU-FP7 gefinancierd onderzoeksproject waarbij TNO slechts beperkt betrokken is.