NW

Physical Sciences

Call for proposals

Cyber Security Research

STW

Enabling new technology

The Hague, juli 2012

Netherlands Organisation for Scientific Research

Contents

1 Introduction

1.1 Background

NWO Physical Sciences and STW hereby invite researchers, representing Public-Private Partnerships to participate in the first cyber security research call by sending project proposals for long term research.

The Dutch government has appointed 9 economic top sectors for growth in its current economic and innovation approach. These top sectors describe a number of themes, ranging from High Tech Systems and Materials to Creative industry and Logistics.

In order to bundle the need for research and innovation in ICT, the Dutch government has ordered the development of a research and innovation agenda for ICT, related to the 9 top sectors. This resulted in the ICT-Roadmap.

This call for proposals for long term cyber security research projects is written within the context of the ICT-Roadmap[1], and is associated with the ICT research and innovation theme '3.1 ICT one can rely on' within this roadmap. This roadman recognises that fundamental and strategic ICT research is crucial for achieving the ambitions of all Dutch top sectors. The National Cyber Security Research Agenda "Trust and Security for our Digital Life" (NCSRA) (http://www.nwo.nl/cybersecurity) could be seen as the implementation agenda of the research and innovation theme '3.1 ICT one can rely on' within the ICT-Roadmap, and forms the framework for this call.

NWO sees it as its task to collaborate with other parties to strengthen the knowledge base for the cyber security industry and to encourage research and the valorization of the results emerging for this for the benefits of the sector.

This call for proposals is a shared initiative of NWO Physical Sciences and STW.. In a government policy document "*Naar de top*"[2] both organisations already announced the development of a research program on cyber security: "*NWO en STW treffen voorbereidingen voor tenminste één PPS-programma over Cyber Security*."

This cyber security research initiative contains a call for long term research (this one) and a call for short term research, making use of the SBIR-instrument (http://www.agentschapnl.nl/content/oproep-sbir-cyber-security).
The call, aimed at long term research, is funded by NWO and STW, and executed by NWO. The call for short term research is funded by four ministries (VenJ, EL&I, BZK, Def) and executed by Agentschap NL.

[1] Roadmap ICT for the top sectors, 2012
(www.ictonderzoek.net/3/assets/File/documenten/Roadmap%20ICT%20for%20the%20top%20sectors.pdf)
[2] Ministerie van EL&I: Naar de top, het bedrijvenbeleid in acties, 13-09-2011

1.2 Available budget

The budget behind this first call for long term research is M€ 3,5. A small part of this budget is reserved for network and valorisation activities in accordance with the ICT-Roadmap. The remaining long term research budget is subdivided into two compartments: a part meant for fundamental cyber security research, and a part meant for applied cyber security research. NWO aims at an equal division of funding over these two types of research.

Within the research projects funded by NWO collaboration with at least one private partner is compulsory, possibly supplemented with other private and/or public or semi-public partners. This partner/ these partners should make a financial and/or in-kind contribution to the realisation of the project. Matching conditions are described in paragraph 3.2.

1.3 Validity of the call for proposals

This call for proposals is valid until de closing date 02-10-2012, 12:00 PM (Central European Time).

2 Aim

The aim of this program is to strengthen long term research in the area of cyber security, The importance of cyber security for our society requires an investment in knowledge generation in this area, and the ultimate delivery of cyber security experts to the Dutch society. Because cyber security threats have multidisciplinary dimensions, also multidisciplinary solutions are needed.

Cyber security is essential for public and private sectors as well as for individual citizens. This is why cybercrime is an important focus area, which is even specifically mentioned in the coalition agreement of the current Dutch government. The way we view cyber security is changing: in addition to the traditional defensive and reactive perspective, a more proactive form of cyber security is receiving more and more attention. It is essential that we safeguard the ICT infrastructure. Very regularly news media report on the enormous damage resulting from security breaches. Security has become a growth market, providing an opportunity for businesses, science, NGOs and governments to gain a head start. This requires expertise that remains up to date so as to be able to deal with the current problems and challenges in the Netherlands, including passports, public-transport smartcards, electronic patient records and energy metres. The perspectives on security and privacy vary among different countries. This field is of particular significance to the Netherlands as a consequence of the country's exceptionally high broadband-Internet penetration rate. Cyber security research projects contribute to the development of knowledge in the Netherlands, with the goal of strengthening the defence against IT disruptions and cyber-attacks and of staying alert. Findings of such research will create commercial opportunities worldwide.
(Long term) Cyber security research spans a broad range from applied to fundamental, from focussed to broad (multi-disciplinary) research.

The research topics as identified by the NCSRA, and extended by one extra topic, together form the scope of this call.

Research questions in the area of cyber security are manifest in a variety of different application areas in which ICT plays an increasingly vital role: home computing, commerce, industry (so-called SCADA systems), the financial sector, e-government, and defence. In connection with the two comprehensive targets of "**security and trust for citizens**" and "**security and trustworthiness in the ICT infrastructure**", the NCSRA identifies the following research topics:

1. identity, privacy and trust
2. malware
3. forensics
4. data and policy management
5. cybercrime and the underground economy
6. risk managing, economics, legislation
7. secure design and engineering

Especially within the Ministry of Defense there is a strong interest for another research topic:

8. Operational cyber capacities

The policy objectives behind this first call are listed in Annex 6.5.
A description of the above mentioned research topics is given in Annex 6.6.

3 Guidelines for applicants

3.1 Who can apply

Applicants of proposals should be employed at a research institute recognised by NWO. The NWO Regulation on Granting (www.nwo.nl/regelingsubsidieverlening) Article 1.1.1 states from which organisations a proposal to NWO can be submitted. In principle these are Dutch institutions for academic education and research and/or researchers from institutes recognised by NWO.

Project proposals are expected to be prepared by a consortium, i.e. Public-Private Partnership. An application for project funding can only be submitted, on behalf of the consortium, by a professor, associate professor (UHD) or assistant professor (UD) employed at one of the above mentioned organisations. Researchers with a tenure track appointment[3] at one of the above mentioned institutions are also allowed to apply as main applicant.
The main applicant should:

- have at least a PhD,
- have sufficient research experience,
- be in a position to remain effectively involved in the research to which the grant application refers for the duration of the period for which the grant is being requested.

The main applicant will be responsible for both the scientific coherence and the results and reporting of the financial results of the project.

Each project consortium must include at least one knowledge institute, to which the main applicant is connected, and at least one consortium partner other than a knowledge institute, e.g. from the profit or non-profit sector, acting as a co-applicant. The consortium (main applicant, co-applicants, consortium partners), is expected to provide co-funding as matching to the NWO grant of the proposed research project.

At most, applicants can apply twice, but only once as main applicant in this call. This means (a) the applicant acts as main applicant for one proposal and as co-applicant for another proposal or (b) the applicant acts as co-applicant for two different proposals.

NWO defines co-applicants as partners requesting NWO funding for scientific research. Co-applicants should be employed at one of the research institutes recognized by NWO.

NWO defines consortium partners as partners within the research consortium, providing either in-kind or cash co-funding as matching to the requested funding of the main applicant and co-applicants. There is no limit to the number of project proposals consortium partners are participating in.

TKI allowance

[3] NWO defines a tenure track appointment as an appointment for experienced scientific researchers with prospects on a permanent contract and a professorship on the long term.

To encourage companies to participate in research consortia in this call, the government (Ministry of Economic Affairs, Agriculture and Innovation) will introduce a TKI (Top Consortium for Knowledge and Innovation) allowance in 2013. This measure is currently being worked out. For every euro that a company invests in a TKI the government will invest a further 25 eurocents. That will not go to the company but to the TKI, where it will be invested in extra research and innovation that the company, in turn, will benefit from (www.rijksoverheid.nl/onderwerpen/ondernemersklimaat-en-innovatie/investeren-in-topsectoren/topconsortia-voor-kennis-en-innovatie-tki-s).

3.2 What can be applied for

This call is meant for long term and strategic research. Researchers formulate research questions in cooperation with the consortium partners for mid- and long term research. NWO finances research being done by knowledge institutes (as described in paragraph 3.1), and requests (in kind or cash) matching by consortium partners of at least 30% of the total research budget (see also paragraph on co-funding). Applicants can apply under the following conditions:

- The project should at least employ one PhD or postdoc for a period of at least two years.
- The maximum amount of project subsidy that can be requested is € 500.000 and the maximum total project budget is € 1.000.000. The maximum co-funding is 50% of the total project budget. The minimum required co-funding is 30% of the total project budget.

The grant can be used for:

- Temporary personnel (junior researcher, PhD and postdoc). In the case of a junior researcher the budget requested will be assessed against experience and the type of activities. The personnel costs will be funded in accordance with the most recent version of the *Agreement for Funding Scientific Research*.
- Temporary non-scientific personnel, for example a student assistant, to support the project. The personnel costs will be funded in accordance with the most recent version of the *Agreement for Funding Scientific Research*.
- Material costs that are directly related to the project, such as the costs of knowledge transfer, valorisation and costs for internationalisation.

Costs for computers, standard software and other costs that belong to the standard facilities of universities, research institutes, studios or labs are not eligible for funding. General costs for project management and coordination are also not eligible for funding. Neither can these be entered under the matched funding.

Simultaneous submission of identical or highly similar proposals is not permitted.

Conditions for co-funding

Co-funding, i.e. contributions by research consortium partners can be either in-kind or in cash. The budget for long term cyber security research, and subject for this call, will be divided into a part meant for **fundamental cyber security research**, requiring at least 30% in-kind matching, and a part meant for **applied cyber security research**, requiring at least 15% in-kind and at least 15% matching in cash. A cash contribution from the private sector demonstrates the willingness to also financially participate in research projects beneficial to all members in the Public-Private Partnership. Furthermore all cash contributions together determine

the TKI-allowance the TKI-ICT is getting to invest in new research projects within this domain.
NWO aims at an equal division of funding over fundamental cyber security research and applied cyber security research.

NWO accepts personnel input and the material contributions as in-kind co-funding under the condition that these are capitalised and they form an integral part of the project. This should be made clear in the description and the planning/phasing of the research proposal. Certain tariffs apply as indicated below (for junior and senior researchers). Note that in-kind co-funding contributions are binding, and should be accounted for in progress reports of the research project.

Co-funding, to be provided by consortium partners, must be confirmed in a 'letter of support'. The letter should contain an explicit statement of the pledged financial or capitalised material or personnel contribution. The amount stated in the letter of support should agree with the amounts put forward in the budget. Letters of support should be addressed to the main applicant and should mention the title of the proposal explicitly. After the research proposal has been approved, NWO will ask the co-funders for confirmation on the co-funding ('confirmation of the commitment by third parties') and, in relevant cases, lay down further arrangements in an agreement.

Requirements and accountability for co-funding

- The research partners and data partners[4] in the consortium contribute a minimum of 30% and a maximum of 50% of the total expenses of the project, either in cash or in-kind;
- In-kind contributions need to be capitalised. Examples are: providing personnel, data, facilities, equipment, etc.
- For in-kind matching by consortium partners, NWO accepts the following integral cost tariffs for a maximum of 1.650 hours a year:
    - A senior-researcher tariff of € 116 an hour, applicable to all personnel with a Masters- or corresponding degree.
    - A junior-researcher tariff of € 81 an hour, applicable to all personnel with a Bachelors- or corresponding degree.
- All in cash matching by consortium partners should be justified in the project application, in the "Requested budget" paragraph.

A more detailed explanation of the required contributions is given in Annex 6.1.

3.3 When can applications be submitted

The closing date for the submission of proposals is **02-10-2012,** 12:00 PM hours CET.

Further information about the procedure can be found in Chapter 4.

[4] Research partners are actively participating in research within the context of the research proposal. Data partners are participating as providers of data being subject of the research.

3.4 Preparing an application

All proposals must be drafted in English, in order to make them accessible to international reviewers. The proposal needs to stand on its own, and all references to internal literature should be avoided. Only references to open accessible literature are allowed. When a reference to a pre-print is unavoidable, a copy of the pre-print should be included in the application, for access by the reviewers.

Your grant application has two parts: a *fact sheet* and an *application form (Annex 6.3)*.

- You prepare and complete the fact sheet directly in NWO's electronic application system Iris.
- An outline of the application form is included in this call for proposals, in Annex 6.3. As soon as you have completed your application form, this should be added to the Iris fact sheet as a PDF file.

3.5 Specific conditions

For proposals for a grant from NWO, the *NWO Regulation on Granting* (www.nwo.nl/regelingsubsidieverlening) applies as equally the *Agreement for Funding Scientific Research* (www.nwo.nl/akkoordbevestiging).

NWO Code of Conduct on Conflicts of Interest
http://www.nwo.nl/codeNWO's Code of Conduct on Conflicts of Interest applies to all persons and NWO personnel involved in the assessment and decision-making procedure of this call (www.nwo.nl/code).

Intellectual property rights (IPR) and knowledge transfer
NWO has a regulation for Intellectual Property Rights (IPR) and knowledge transfer. If a researcher submits a proposal on behalf of an institution recognised by NWO then the project partners must confirm that they have taken note of the IPR and knowledge transfer regulation as described in the Appendix IPR regulation NWO - creative industry (see Chapter 6: Appendices, 6.3).

3.6 Submitting an application

An application can only be submitted to NWO via the Iris system. Applications not submitted via Iris will not be admitted to the selection procedure. A main applicant is obliged to submit his/her application via his/her own Iris account.

If the main applicant does not have an Iris account yet then this should be created at least one day before the submission. Then any possible registration problems can still be solved on time. If the main applicant already has an Iris account then he/she does not need to create a new account to submit a new application.

For technical questions, please contact the Iris helpdesk, tel. +31 900 696 4747.

4 Assessment procedure

4.1 Procedure

The first step in the assessment procedure is to determine the admissibility of the application. This is done using the conditions stated in Chapter 3 of this call for proposals.
The NWO Code of Conduct on Conflicts of Interest applies to all persons and NWO staff involved in the assessment and/or decision-making process.

The program office will process full proposals submitted, when the requirements of this call are fully met. This means that:

- the application form was fully and correctly completed, or the applicant responded in time to a request to rectify the situation,
- the application was submitted by a professor, associate professor (UHD) or assistant professor (UD) employed at one of the knowledge institutes mentioned in paragraph 3.1 on behalf of a consortium,
- the application is consistent with the objective of the program,
- the application was submitted online via Iris,
- the application was submitted before the deadline,
- the application is consistent with the maximum amount of project subsidy requested and the maximum total project budget, as defined in paragraph 3.2 of this call,
- the application meets the requirements for co-funding as stated in this call for proposals.

If correction is possible, then the applicant will be given the opportunity to correct his/her application within 48 hours. If the application is not corrected within that timeframe, the application will definitely not be taken into consideration. As soon as the situation is rectified and the application can be declared officially admissible, it will be processed.

Assessment of proposals
An independent *evaluation committee* will be asked to assess the full proposals submitted in the Cyber Security research call based on the criteria mentioned in paragraph 4.2. The evaluation committee will consist of around 8 people, and will be a balanced combination of both (international) scientific experts in the research field of cyber security, and relevant members of the private sector (independent representatives of industrial parties, and representatives of social enterprises in the field of cyber security). Two members of the SBIR Cyber Security evaluation committee will be members of this evaluation committee. The evaluation committee will assess all proposals on the criteria, as mentioned in paragraph 4.2.

NWO reserves the right to add a *pre-selection* round to the procedure, in case of a very high number of applications. Pre-selection may be used when the number of applications transcends the number of reasonable acknowledgeable applications by a minimum of four times, in this case 28 applications. In case of pre-selection, the following procedure will be used:

- Proposals will be assessed by the evaluation committee before review by independent (international) peer-reviewers. The evaluation committee will divide the proposals in the categories ‘likely’ and ‘unlikely’. Likely means proposals are likely to end high in the final ranking, and are selected for further evaluation by the review committee. Unlikely means: the research proposal in this form is unlikely to end high in the final ranking.

- The NWO program office will inform applicants on the provisional outcome of the pre-selection. Applicants will get the chance to react on the provisional outcome of the pre-selection. Reactions will be presented to the evaluation committee. The evaluation committee reserves the right to change their opinion based on the reaction of the applicant.
- The evaluation committee will propose the pre-selection to the cyber security steering group, and the steering group determines which proposals are to be rejected in the pre-selection, and which proposals are to be subjected to the full selection procedure.
- All applicants receive a letter informing them on the outcome of the pre-selection. Only the 'likely' assessed proposals will be subjected to the full review procedure. The 'unlikely' assessed proposals will be rejected.

The (full) selection procedure is as follows:

- (Pre-selected) proposals will be subjected to peer-review by at least two, and at most four independent (international) experts. The experts will be requested to review the research proposal on the scientific quality of the proposal, as mentioned in paragraph 4.2. All review reports will be submitted to the applicant and the evaluation committee.
- The valorization/relevance of the proposed research will be assessed by representatives of the evaluation committee, to guarantee their knowledge of the national societal en economic situation.
- The applicant receives the opportunity to react on the review reports on scientific quality, and assessments on valorization and relevance, in the form of a rebuttal.
- The evaluation committee will rank the proposals, taking review reports into consideration, and submit their motivated ranking to the cyber security steering group.
- The cyber security steering group will make the final decision on the granting of research proposals.

Simultaneous submission of identical or highly similar proposals is not permitted.

Successful (i.e. granted) applicants must begin their research within six months after the date of the grant award. In case applicants fail to do so, NWO reserves the right to withdraw funding granted to the applicant.

With effect from 1 January 2012 NWO will use a new qualification for applications assessed. Information about the qualification can be found on the NWO website: http://www.nwo.nl/qualifications.

Provisional timeline for this call for proposals

October 2nd 2012	Deadline submission of proposals
November 2012	(if applicable) Pre-selection of the proposals Consultation peer reviewers
November 2012 – February 2013	
February 2013	Obtaining rebuttals from applicants. On average researchers are given 1 weeks to give a response
March 2013	Advice evaluation committee to the cyber security steering group
April 2013	Decision cyber security steering group
April 2013	NWO informs the applicants about the decision

4.2 Criteria

Assessment criteria for proposals

Applications will be assessed by an evaluation committee on the following two criteria:

- Scientific quality;
- Valorisation/relevance.

The criteria are weighed equally in the ranking process.

Scientific quality indicators:

- Multidisciplinary and international scientific collaboration;
- The potential for innovative research;
- Competence of the research team;
- Research method and approach;
- Theoretical background and framework;
- The plan of work and its feasibility;
- Adequacy of budget and infrastructure.

Valorisation/relevance:

- Contribution to or impact on (one of the) action lines described in the NCSRA;
- Relevance and urgency of the proposed research for scientifically strengthening the cyber security community;
- Economic and/or societal added value of the foreseen research results;
- Composition of the consortium in regards to the valorisation goals of the proposal;
- Level of participation of private and public consortium partners in regards to the valorisation goals;
- Effectiveness of the participartion of consortium partners in regards to the valorisation goals;
- Organization of the project: interaction and cooperation between researchers and private and public partners in the consortium.

5 Contact details and other information

5.1 Contact

5.1.1 Specific questions

For specific questions about Cyber Security Research and this call for proposals please contact
Jan Piet Barthel (j.barthel@nwo.nl, +31 70 3494495) or Joep van Wijk at NWO (j.vanwijk@nwo.nl, +31 70 3494459).

5.1.2 Technical questions about the electronic application system Iris

For technical questions about the use of Iris please contact the Iris helpdesk. Please read the Iris manual before consulting the helpdesk.
The Iris helpdesk is available from Monday to Friday from 11.00 to 17.00 hours on +31 900 696 4747. Unfortunately not all foreign phone companies allow you to phone to a 0900 number in the Netherlands. You can also send your question by e-mail to iris@nwo.nl.

5.2 Other information

The call text and further information related to this tender can be downloaded from the NWO Cyber Security website: www.nwo.nl/cybersecurity. See also paragraph 3.4.

6 Annexe(s):

6.1 Arrangement for in-kind contributions by private parties in the Cyber Security Research program

Definitions

1. Private parties

Private parties are defined as businesses. NWO understands a business to be: an organisational association unit or person focussed on sustained participation in the economic system with the aid of labour and capital and with a profit motive. SMEs fall under this category.[5]

2. Public and semi-public parties

Public and semi-public partners are defined as knowledge or other institutions that are not one of the knowledge institutions recognised by NWO (such as universities of applied sciences, heritage institutions, municipalities, intermediary organisations or foundations) and which do not belong to the category private parties.

Provisions

1. Possibility of participation in NWO research by private parties with in-kind contributions

Private parties and public or semi-public parties can participate in NWO research programs by means of a financial contribution to the program budget or project budget which NWO allocates to research groups of knowledge institutes to carry out an approved research proposal.
Private parties can participate in the NWO research program with a partial in-kind contribution under the following conditions:

a. The total private contribution to an NWO research project in the Cyber Security Research call should be at least 30% of the project budget approved by NWO, and a maximum of 100% of the funding requested by the knowledge institute;
b. in-kind support / efforts must:
   - be essential to the project;
   - be included in the NWO-approved budget of the research costs of the project application in which the private party participates (see provision 3 for permitted in-kind contributions) and must fall within one of the cost categories referred to under 3 a through c.

2. Commitment

If a private party participates in the research project with a partial in-kind support as described above, the private party will commit itself to NWO for the in-kind support as well as the financial (in cash) support. NWO will invoice the promised financial (cash) contribution in semi-annual instalments.

3. Permitted in-kind contributions

The following costs, directly attributable to the research project and incurred by the private party, may be contributed by private parties as in-kind contributions (see also provision 1):

[5] The SME definition from the European Commission is used. An SME is understood to be a business that has fewer than 250 employees, a turnover of less than 50 million euros and a total balance of less than 43 million euros. Consideration should also be given to participations (⩾25%) in and from other businesses that affect the autonomy of the business. Documentation: DG Enterprise, http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm.

a. Hours worked within the scope of the project:
   - wage costs, it being understood that these are based on an hourly wage, calculated on the basis of the annual wage at full employment according to the column *income for income tax* of the wage statement, plus the surcharges for social contributions payable by law or under individual contract or collective bargaining agreement, and based on 1.650 productive hours per year. This amount may be increased with a surcharge for other general costs, subject to a maximum of 50% of the wage costs referred to above. The ensuing hourly rate to be attributed to the project, including said 50% surcharge for general costs, is capped the tariff as mentioned in paragraph 3.2 in the call for proposals. Contribution of costs for supervision or for project management is possible in the event of active participation of the intended supervisor or project manager in the research project (cf. under 1b of this annexe).

b. Costs of material and resources to be used, based on the original purchase prices, distinguishing between products owned by the co-funder (list price) and products from other companies, bought by the co-funder (purchase price).

c. Use of equipment and machines
   - Costs associated with the purchase and use of machines and equipment, it being understood that these are based on the depreciation costs to be attributed to the project, calculated on the basis of the original purchase prices and a depreciation period of at least five years; costs of consumables and maintenance during the period of use.
   - Costs of purchase and use of machines and equipment that were not purchased solely for the project will only be considered project contributions pro rata based on the foregoing if there is a time log for each machine or for the equipment that conclusively establishes the operating hours.
   - In-kind contributions in the form of a discount on the regular purchase price in economic transactions (list price) of machines and equipment. The discount must be at least 25% of the list price. The costs charged to the project's equipment budget will then amount to the list price less said discount. When there is no list price a discount is not accepted.

4. <u>Accounting of in-kind contributions</u>

Private parties must render account of their in-kind contributions to NWO by means of a statement of the contributed costs, to be provided to NWO within three months after the end of the research project to which the in-kind contribution was made. The application for approval of the in-kind contribution must be submitted simultaneously with the application for approval of the subsidy amount by the university partner(s), accompanied by a collective final report. If the in-kind contribution for which account must be rendered exceeds € 125,000, an auditor's report must be submitted; in other cases, a written statement by the holder of a power of attorney stating that the contributed in-kind efforts can actually be attributed to the project will suffice.

If the private party, that committed itself to a research project with an in-kind contribution, ultimately fails to make such in-kind contribution in full or in part, or cannot render account of the same, NWO will invoice this private party for such part or the full in-kind contribution, so that the total contribution as undertaken is honoured.

6.2 IPR and knowledge transfer arrangement NWO Research Projects

- *General*

When submitting a project proposal within the scope of the NWO Research Projects of the Cyber Security Call, the project parties shall confirm that they have taken note of the IP and knowledge transfer arrangement described in this document. Before a granted project commences, the project parties will enter into a Project Agreement with NWO regarding IP and knowledge transfer, as well as regarding other matters such as finance, progress reviews and confidentiality (*vide* the Project Agreement model that will be available on the site in due course).

The conclusion of a Project Agreement between NWO and the project parties is one of the conditions to which the grant of a subsidy for the relevant project is subject.

- *Background Information*

The parties participating together in a research project shall provide NWO with a written statement of the background knowledge they wish to make available for use in a project before the project commences. NWO will include the statements obtained from the parties in an annex to the Project Agreement to be concluded. During the project, additional background knowledge may be contributed in an analogous manner.

Any contributed background knowledge remains the property of the contributing party (hereinafter: the Provider) and may be used by the receiving party or parties solely for the purposes of the project within the context of the objectives of the research. Upon written request, the Provider shall make the necessary background knowledge available to the requesting party at no cost by means of a non-transferable, non-exclusive licence for the duration of the project. In this respect, the Provider shall in good faith provide the receiving party/parties with all relevant information on the background knowledge in question, including a statement that the knowledge is free of third-party claims, or, if such claims exist, what restrictions apply to the use of the knowledge and any further exploitation of such knowledge.

- *Foreground Knowledge -- Results*

Initially, the Results within a research project accrue to NWO. In this process, NWO acts as an intermediary and does not aim for a patent portfolio itself. If an invention is made within a project, the participating project parties shall have the first right of refusal to (cause to) protect this invention in their name and at their expense and subsequently obtain a patent on said invention in consideration of fair market compensation to NWO. The guideline for the maximum amount of compensation is formed by the project costs or sub-project costs incurred that led to the invention in question, minus the relative private contribution to said costs. The parties shall negotiate with NWO about the definitive amount of compensation and the stages, if any, of payment, and reach agreement on these issues within four months after the negotiations commenced, after which a patent application can be filed. SME parties may obtain a discount on the compensation payable by setting off the costs for obtaining IP against the compensation to be agreed. The compensation will be routed, via NWO, to the project party concerned where the invention was made for further research for the purposes of the subject/program.

If multiple project parties are interested in (causing) the protection of the same invention and obtaining a patent, they will mutually agree, if possible even before the project commences, which party or parties will be the ultimate proprietor(s). If no agreement is reached in this respect, NWO will decide with regard to the right to patent the invention after separate consultation with the project parties involved.

- *Publication of Results*

The project parties shall not publish or otherwise disclose results, other than with the other project parties' consent. The parties involved shall respond in writing within 4 weeks after the request for publication. If the parties have not responded in writing within this period, this may be considered

consent. Within two months after the publication request, the parties may require changes in order to protect their interests with regard to the patentability of the results, however without jeopardising the scientific integrity of the publishing party. If the results give rise to a specific possibility for a patent application, the publication may be suspended for no more than nine months after the request for publication in order to give the opportunity to protect the results.

6.3 Research proposal application form

On submission of your application in Iris, you will be requested to complete a factsheet. The application should be included as an attachment in Iris, in PDF format.

1a Project Title
The title of the research project for which funding is requested. This should be brief but as specific as possible, and must correspond with the title given on the factsheet.

1b Project acronym
(Where applicable) This must also correspond with the information given on the factsheet)

1c Principal applicant
Give only the name of the main applicant (who also acts as the contact person and is the intended project leader).

1d Application history
State whether this is an entirely new proposal or (an amended version of) a proposal which has been submitted on one or more previous occasions. Proposals which have been assessed and rejected in the past must have achieved at least a 'Category B' rating to qualify for re-assessment in the current round. Applications which achieved a 'Category C' rating may not be resubmitted in the same form. (The rating given to your previous proposal is shown in the rejection letter).
If you have submitted a previous application in respect of this research project, or a project which is substantially similar, and that application was declined by EW or another competent assessment body, you should indicate which part(s) of the proposal have since been amended. Please state the reference (dossier number) of the proposal (as shown on the relevant correspondence).

2a Scientific summary
A brief summary (maximum 250 words), in **English**, written for specialists in the relevant research field. This should correspond exactly with the summary given on the factsheet.

2b Abstract for a lay readership (in Dutch)
Include a summary (maximum 500 words) in **Dutch**, written for the benefit of researchers in other disciplines and a lay readership. This summary should not be a direct translation of the English scientific summary. It should include:

- a clear explanation, in simple language, of the nature and content of your proposal;
- an account of past work in this area;
- an account of what you intend to do, and why this is important;
- an account of the expected results;
- an account of why your research may be deemed innovative.

If a grant is awarded, NWO may use this summary for publicity purposes.

2c Keywords
List up to six relevant keywords.

3 Classification
List the (sub)disciplines applicable to the research project. Classifications could be:

- Computer Science (a specific research field or subdiscipline may also be stated).
- Mathematics (reference may also be made to the Mathematics Subject Classification 2000 at http://www.ams.org/msc).

You may also list an alternative discipline, such as 'economics' or 'law', if you believe that your proposal falls under this heading.

4a Members of the research team

List those persons who will be directly involved in the research project, including the holder of the position for which funding is being requested. Where possible, state all surnames, initials, titles, specialisms and the university or institute with which the researchers are affiliated. This information should be presented in the form of a table. If the research is to be undertaken as a PhD project, give the name of the supervisor. The evaluation committee will encourages proposals submitted by female main applicants.

Individual CVs should not be attached, but you may include links to personal websites or a brief description (no more than half an A4 page) of the team as a whole. Referees will be asked to assess the competence of the research team (see also Section 4.2, 'Criteria'.)

4b Participating partners

List all consortium partners (other than the main applicants organisation) participating in the research project. For each partner, give a short description of the partner, describing:

- The type of organisation;
- The size of the organisation;
- The sector the organisation is active in;
- The role of the organisation in the research project;
- The contribution of the research partner in the project;
- (if possible) the participating people in the organisation.

5 Type of research

Indicate and clarify whether the type of research proposed is fundamental cyber security research, or applied cyber security research.

6a Description of the proposed research

In this section, state or describe:

- The scientific research question ('terms of reference') and the intended results or outcomes.
- The research approach and methodology.
- The scientific importance and urgency of the proposed research.
- The relationship between the proposed research project and any similar or complementary research which is being conducted elsewhere.
- The relevance of the proposed research to that currently being performed by the group(s) which the funded researcher will join.

6b Multidisciplinarity

State the degree to which your research project can be deemed multidisciplinary. Will you, for example, be using approaches or methods drawn from other disciplines? Will your project result in any innovation within other disciplines?

Word count: please state the number of words used in section 6. The maximum number of words is 3.000 words.

7. Valorisation and relevance

7a Valorisation

In this section, please describe:

- Level of participation of private and public consortium partners;
- Organization of the project: interaction and cooperation between researchers and private and public partners in the consortium.

7b Relevance

In this section, please describe:

- Contribution to or impact on (one of the) action lines described in the NCSRA;
- Relevance and urgency of the proposed research for scientifically strengthening the cyber security community;
- Economic and/or societal added value of the foreseen research results;
- Effectiveness of (the contribution to) the proposed service or product for the goal of the research.

Word count: please state the number of words used in section 7. The maximum number of words is 2.000 words.

8 Project planning

Phasing

Indicate the phasing of the entire project. What specific tasks can be identified and how are they to be scheduled over time?

Education and training

The purpose of funding a research position is not only to facilitate the proposed research, but also to contribute to the training and education of the holder of that position. In this section, you can describe any special aspects of the project which will serve this aim.

9a Literature (internal)

List the five most important publications produced by members of the research team and which are relevant to the research proposal.

9b Literature (external)

List the references and sources used in preparing the proposal.

10. Requested Budget

10a Requested personnel budget

Describe the budget requested of NWO for personnel costs regarding the research proposal. NWO only accepts budget requests for scientific personnel, working for one of the knowledge institutes mentioned in paragraph 3.1 of this call for proposals.
Personel costs are subsidised in accordance with the most recent 'Agreement on Employers' responsibilities NWO-VSNU.

10b Requested additional budget

NWO allows applicants to request additional funding for travel costs, costs for new investments related to the research proposal, and costs related to knowledge transfer. Please describe the requested additional budget, and describe the relevance of the additional budget in relation to the proposed research.

10c Co-funding of the consortium partners

10c.1 In-kind co-funding

Give a description of the amount of in-kind co-funding of each (in-kind co-funding) consortium partner.

10c.2 Cash co-funding

Give a description of the amount of cash co-funding of each (cash co-funding) consortium partner, and describe how the cash co-funding will be used in the project.

10d Total project budget overview

Please give a total project budget overview of the proposed research, including the in-kind and in-cash contributions of consortium partners, and the personnel and additional budget requested of NWO.

6.4 Cyber Security Research and Top Sector Policy

The Dutch government policy is headed towards relating research grants to so called top sectors. In this Annex the cyber security research challenges as formulated in two current roadmaps are repeated.

From de ICT-roadmap (instances of high potential ICT-innovation in top sectors):

As our reliance on the ICT infrastructure increases, so do concerns about its security. The growing complexity of ICT systems means that bugs and vulnerabilities are harder to avoid, creating new opportunities for increasingly sophisticated attackers. The recent attack on a uranium enrichment facility in Iran by the Stuxnet worm shows that strategic interests can attract cyber-attackers. ICT security issues are no longer limited to traditional computer systems, such as PCs and laptops. Rather, they surface everywhere, from electricity and water supply systems to the health service, from public transport to smart cars, from implants to supply chains, and from banking and logistics to the emergency services. Trust is a *conditio sine qua non* for normal economic transactions and inter-human communication. It is at the core of social order and economic prosperity, and in an increasingly ICT-dependent world, the security of ICT plays an ever more important role here. Addressing cyber security involves many domains of expertise, or disciplines. We do not just need technical expertise to detect and stop attacks - or better still - prevent them. We also need laws and regulations that better cope with computer crime, and we need to better understand the forms and causes of cyber-crime, the effectiveness of measures, including law enforcement, the underground economy, and to see where economic drivers for implementing security measures are lacking and regulation may be needed. Relevant industries are banking, industries operating in the critical infrastructure and utilities.

Prerequisite to provide ICT-services safely and reliably and how to use them with confidence is confidence in ICT itself. With the growing use of ICT, confidence is undermined by disruptions of networks, services, applications and abuse of ICT, for example in the form of botnets (a network of infected PCs), viruses or breaches of security with personal data. Therefore, Cyber security is a generic theme for supporting secure use of ICT.

Security is a multidisciplinary field that cannot be approached from the technological viewpoint only, and requires consideration for human, regulatory, and legal aspects as well. Specific topics covered in the National Cyber Security Research Agenda (NCSRA) are: identity, privacy and trust management, malware, forensics, data management, cybercrime, risk management, and secure design. The topics range from scientific study to tooling and engineering. The NCSRA has been adopted by the Dutch Cyber Security Council. Under the umbrella of this agenda several research programs will be proposed with stakeholders who have demonstrated their support to the agenda both in the private and public sectors and ranging from applied to fundamental use-inspired research. Specific technical and scientific challenges include improving malware detection, prevention and removal. Also, finding usable solutions for privacy preserving identity management and for usage control of sensitive data and improving forensics tools and implementing accountability of users in distributed systems are key elements. And, improving the security of the critical infrastructure as well as analysing the economics of security and the evolution of cybercrime. Realising security and privacy by design as well as better tools supporting writing secure software and analysing the security of software and hardware is important too. Finally, it is important to study the link between cyber-security, economics, risk management and regulations and the secure exchange of business information and administration: e-recognition, for example.

From the Roadmap HTSM Security (one of the 14 roadmaps under the top sector HTSM)**:**

Our society is becoming increasingly dependent on ICT. Therefore, the protection of our vital ICT infrastructure is a matter of national security. Due to the ever increasing vulnerabilities and the

rapidly changing pernicious threats, cyber security is becoming increasingly important for businesses, vital sectors, the government and individuals.
Combating cybercrime is an explicit focus of the current government. The government has drafted the National Cyber Security Strategy (NCSS) for an integrated approach to cyber security. Overarching objectives are public confidence and resilience of the vital infrastructure. As part of this, the Cyber Security Council, consisting of representatives from the government, the corporate sector and science community, was established to advise the government and to provide private parties with solicited an unsolicited advice in the area of digital security. Another important component of the NCSS is the National Cyber Security Research Agenda (NCSRA)[6].

The NCSRA distinguishes the following research topics:

- identity, privacy and trust
- malicious software
- forensics
- data and policy management
- cybercrime and the underground economy
- risk management, economy and legislation
- secure design & engineering

The NCSRA distinguishes the need for shorter-term, applied research to quickly identify security problems and solutions, and the need for long-term research as in-depth investment in knowledge in this area with (embedded) training of more qualified staff with expertise in cyber security being an important spin-off effect.
In June 2011 the Cyber Security Council approved the NCSRA and gave "IIP Veilig Verbonden" the task to prepare a specific research program and to provide a framework for the organisation and financing.

[6] National Cyber Security Research Agenda: "Trust and Security for our Digital Life".
http://www.iipvv.nl/IIP-VV-kanaal/IIPVV-Downloads.html

6.5 Policy objectives behind the (first) tender for Cyber Security Research

1. Improving the security and the reliability of the ICT infrastructure and ICT services.
2. Anticipating on future cyber security-challenges in the Netherlands, by developing knowledge aimed at prevention of cyber-attacks and averting of threats.
3. Stimulating the Dutch cyber security economy and advancing innovation in this sector.
4. Strengthening and broadening the knowledge base in the field of cyber security.
5. Connecting research initiatives in the field of cyber security.

Elaboration on policy objectives

1. Improving the security and the reliability of the ICT infrastructure and ICT services
Central for a secure ICT infrastructure are:

- Continuity of the network- and information structure, for both land-based and wireless infrastructures;
- Tenability/vitality of the network and information infrastructure, both in national and international context (through cooperation with international partners);
- Providing information to end-users in relation to perspective for action, in order to raise and to keep/maintain the awareness of a safe and trustworthy use of ICT and telecom, at a high level.
- Intrinsic security of the currently applied software and hardware, for the purpose of both networks (infrastructure) and services.

Behind all efforts in this area is the general objective that citizens should experience a justified trust in the use of the ICT infrastructure. In the international perspective, the Netherlands aims at obtaining a leading position in this field of expertise. The scope should be focused at both prevention and response.

2. Anticipating on future cyber security-challenges in the Netherlands, by developing knowledge aimed at prevention of cyber-attacks and averting of threats.
The complexity of ICT infrastructures and our growing dependency of these infrastructures leads to new vulnerabilities for misuse and disturbance. Cyber-espionage, cybercrime, cyber terrorism and cyber warfare, as well as inadvertent disturbance by technical or human failure or natural cause can cause great damage or can result in societal disorder. These are threats which develop at a rapid pace, and the solution to these problems is knowledge intensive.
Because of the increasing digitisation of our society, it is of high importance to address cyber threats both in the short, as well as in the long term. This concerns for instance the development of 'situational awareness in cyberspace' and the possibility to determine the attribution of cyber-attacks, but also developments like 'security by design' and the timely acquisition of high quality threat and risk analysis. In this regard, the following action lines have been described in the National Cyber Security Strategy (NCSS):

- Increasing the defensibility of the vital infrastructures;
- Enhancing the response capacity in order to avert ICT interferences and cyber-attacks;
- Intensifying the investigation and prosecution of cybercrime;
- Developing threat and risk analyses.

3. Stimulating the Dutch cyber security economy and advancing innovation in this sector
Cyber security, and in particular the NCSRA, is associated with the top sector "High Tech Systems and Materials", and the ICT-Roadmap. Therefore, the (partial) execution of this research agenda will excel this top sector among others.
The knowledge infrastructure of a top sector will be strengthened by actively connecting the Dutch private sector (private R&D) to their research program or roadmap, as well as by stimulating international top talent and foreign private (high tech) companies to settle in the Netherlands. Research in light of "Holland branding" in the field of cyber security falls within this scope.

The Dutch private sector already has an international leading position in the field of contesting cyber threats. The aim is to deepen and broaden the knowledge in this field, in order to maintain our leading position, by focusing on possibilities for innovation. Cooperation in the field of security with parties like TNO Defense, the Netherlands Forensic Institute (NFI), Thales and Fox-IT, contribute to this aim.

The *Bedrijfslevenbrief* of the Department of Economic affairs, Agriculture, and Innovation (Ministerie van EL&I) describes close cooperation between private parties and scientific community as a likely condition for innovation. This is translated in this research tender by the requirement of a 30% participation of private companies in the execution of the research.

4. Strengthening and broadening the knowledge base in the field of cyber security
In order for the Netherlands to stay ahead of (new) cyber threats in the coming decades, investments in knowledge and innovation in this area of expertise is of the highest importance. Fundamental and applied scientific research and stimulation of the development of highly innovative security solutions will result in a higher level of cyber security. High quality education on all levels is important for the continuing development of trustworthy ICT, and to contest new threats. Through close cooperation between the scientific community and the private sector both innovation is promoted in the security domain, and more students are attracted to this area of expertise.

The aim for the coming years is the graduation of 20 PhD students, and 60 master of bachelor students on top of the current numbers in the field of cyber security. Multidisciplinary research will be stimulated in this research tender.

In summary: the research activities within the NCSRA support the action lines of the NCSS, and the broader aim of stimulating research and development in the area of cyber security within knowledge institutes and private companies.

5. Connecting research initiatives in the field of cyber security
Research in the field of cyber security usually takes place within the scope of existing (organisational) structures. Connecting different research initiatives provides possibilities to strengthen these initiatives, and to allocate or bundle the scarce means more efficiently. This broader scope therefore aims at being an instrument able to connect the existing research initiatives in the field of cyber security. Important in this context are the synchronisation with the NCSRA and TNO’s demand driven programs, and actively searching cooperation with the EU research framework and research programming from other governments (i.e. DHS in the US).

In combination with a framework for research, via initiatives resulting from the research agenda, the NCSRA provides the possibilities for researchers and companies with common needs to get in touch with each other, thereby stimulating the connection between the different research initiatives.
The NCSRA also provides opportunities to submit research trajectories in a broader context, making it possible to efficiently adjust needs, actual research and available means.

6.6 Research Topics in the National Cyber Security Research Agenda

'Trust and Security for our Digital Life'

About this document: This document summarizes the research topics as identified in the National Cyber Security Research Agenda, which is available in full from http://www.iipvv.nl/IIP-VV-kanaal/IIPVV-Downloads.html

The **NCSR A**genda identifies two over-arching goals:

Security and Trust of Citizens This includes privacy protection, security of mobile services, data and policy management, and accountability.

Security and Trustworthiness of Infrastructure This includes malware detection and removal, intrusion detection and prevention, trustworthiness of networks and hardware, soft- ware security, security of SCADA/industrial control systems (ICS), and secure operating systems.

Research projects that address these goals can

- target different *research topics* – explained in more detail below,
- target different *applications domains*, and
- range from short-term and more applied research to more fundamental research, as illustrated in figures 2 and Fig 1.
  Tackling cyber security is not just a matter of technical IT expertise. It requires collaboration between very different communities and *disciplines*:
- the *β* disciplines of computer science and engineering, and neighboring areas of mathematics (notably cryptology) and electrical engineering.
- the *α* and *γ* disciplines of law, criminology, (business) economics, (information) management, applied ethics, psychology and sociology.

To structure the discussion on a potentially infinite list of research topics, the **NCSR A**genda distinguishes the following research topics:

1. Identity, Privacy and Trust Management

Managing the (digital) identities, protecting user's privacy and managing the trust in the online world are essential functionalities of the future internet[1] , which are required in each of the application areas listed above. The application areas concern important but distinct aspects of the digital life of the citizen. In each of these, different authorities, and different numbers of authorities – sometimes one (e.g. the government), sometimes many, sometimes none – will be responsible for providing and controlling identities, and different authentication mechanism will be used. Therefore, different identity management solutions are needed to cater for the various needs. Research sub-areas include the computer science and crypto techniques; to ensure privacy and to handle identities securely, organizational rules and guidelines to delegate trust, and rules and legislation to deal with identity theft, privacy and anonymity rights, as well as private date retention and corresponding access rights.

1 See Future Internet Assembly: http://www.future-internet.eu/

Figure 1: Application domains and research topics

2. Malware

Malware, short for malicious software, denotes all forms of hostile, intrusive and annoying software or program code. The ability to run malware is essential for many types of attack. Serving as a *condition sine qua non* for generating social and economic power for the attackers.
Thus, the threat of malware will remain critical for the foreseeable future. Currently, we experience the threat of malware most saliently in the form of botnets –millions of infected machines tied together in networks at the disposal of attackers. But malware evolves with the ICT infrastructure. We are already seeing malware on social networks, in cloud computing and on mobile devices.
In terms of research, it poses an interdisciplinary challenge. We need advances in technology, as well as arrangements to shape the socio-economic forces that fuel or mitigate the spread and impact of malware. Unless these issues are researched jointly, we will be stuck with partial solutions of limited value.
Technological advances include attack detection and prevention, incident recovery, reverse engineering, and attack analyses. For instance, to detect and prevent attacks, we need techniques and tools to spot and remover vulnerabilities from software, and monitoring systems to raise an alarm when a program behaves in a anomalous manner.
Analysis of malware requires reverse engineering techniques to help us understand what it is doing, as well as methods to estimate the number of infected machines and the effectiveness of counter-measures. From an historical perspective, we should study trends in malware-as doing so prepares us for new threats in time.
While originating in criminal behavior, the magnitude of the malware threat are also influenced by decisions and behavior of legitimate market players such as Internet.

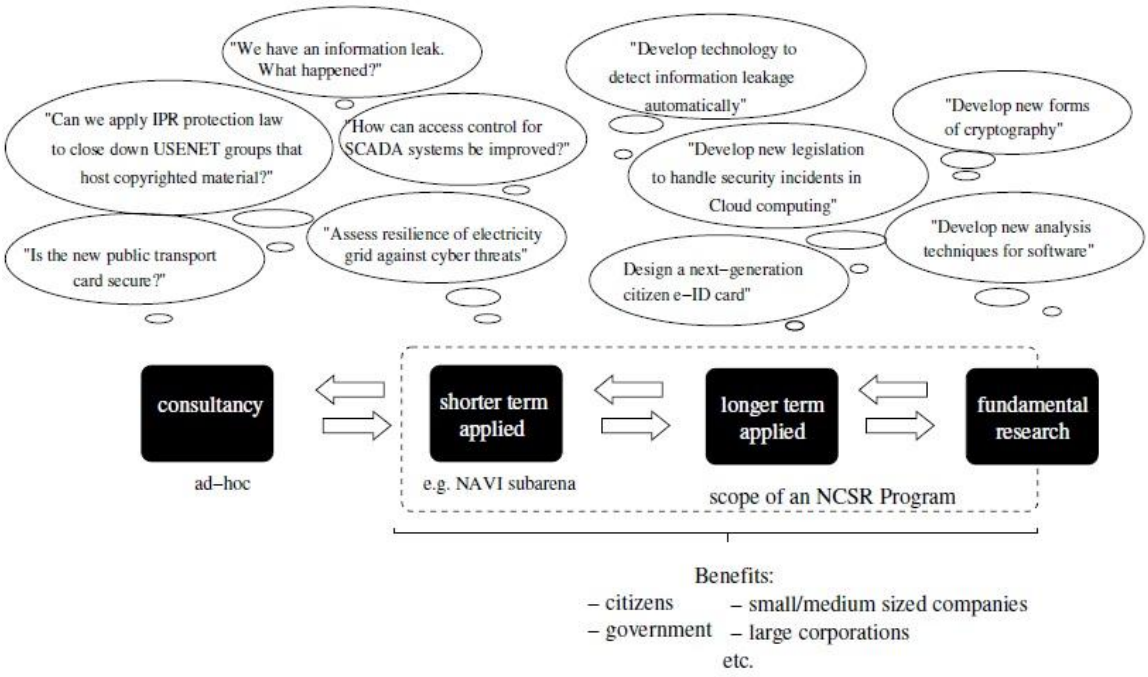

Figure 2: The spectrum of ICT security research problems – with examples

Service Providers (ISPs), software vendors, e-commerce companies, hardware manufacturers, registrars and, last but not least, end users. Here, critical questions focus on economic incentives for the variety of market players. These can be shaped by self-regulation, state regulation and liability assignment. At the organizational level, we need policies to govern the management of hardware and software (including purchase, configuration, updates, audits, decommissioning), and guidelines regarding the management of information.
In addition, we often lack understanding about the socio-cultural context of the malware. Why is it doing what it is doing? The threat posed by Anonymous (the loose group of citizens and hackers that attacked companies that interfered with WikiLeaks) is very different from that of criminal organizations herding massive botnets, and that of state-sponsored cyber espionage and warfare. Studying the origin of attacks and the nature of the victims, as well as the language and socio-cultural references in malware help linguists and sociologists to profile the attackers.

3. Forensics

The goal of cyber forensics is to examine digital media in a sound manner to identify, preserve, recover, analyse and present facts and opinions about the information. Forensics, and, more generically, Computer Security Incident Response (CSIR), is an important part of cyber security. It operates on the corrective or repressive side of security, i.e. it comes into play after a security breach has occurred and attempts either to correct the problem as quickly as possible, or to find evidence to be able to identify and prosecute the culprit.
The first decision after an incident is an economic one. How essential is the compromised system? For example, in a critical infrastructure setting such as a power station, it may be more important to get things up and running (without running the risk of a repeat) than to gather forensic evidence. If, however, the decision is made to consider the compromised system a crime scene, highly skilled digital forensics expertise is needed on-site as quickly as possible to collect evidence, in a way that provides evidence that is admissible in a court of law. This process requires deeply technical as well as legal knowledge. Legal expertise about digital forensic evidence is also very important in getting more visible cases where cybercriminals are successfully prosecuted. Live forensics (forensics on a system that cannot be switched out, as in critical systems) and the attribution question (linking the criminal activity to the criminals behind it) are examples of issues that urgently require additional research. Forensic evidence has been used in a number of high profile cases and is becoming widely accepted as reliable within US and European court systems. However, this may be hampered by a

lack of official standards for digital forensic evidence, especially with multiple parties providing digital forensic evidence.

4. Data and Policy Management

In the application areas a variety of data plays a key role. However, the confidentiality, availability, authenticity and integrity requirements for different kinds of data can vary greatly, both in the technical as well as in the legal sense. For example, health records must be kept for 70 years, and therefore require strong security, whereas other data is almost ephemeral, such as the data kept by RFID tags. In this area, we need computer science research to develop data management techniques, but also organizational procedures, to ensure correct handling of sensitive data, and research to make sure that technical policies match with the user's mental models and understanding.

5. Cybercrime and the underground economy

There is organized cybercrime, such as skimming, botnets, provision of child pornography and advance fee fraud, and unorganized (common) cybercrime, such as simple frauds, down- loading child pornography, uttering threats, etc. In both cases we need to understand the (explaining) factors that lie behind the crimes, the modus operandi and the criminal careers of cyber criminals, and, in the case of organized crime, how their organizations work. We need to know more about patterns in cybercrime, who the victims are and how victimization can be explained. Since money (and as a result of that goods and information with a monetary value) is a key factor in many crimes, it is important to better understand the underground economy, its size, its characteristics and how it is intertwined with the legal economic system. Also we need to know more about the effectiveness of measures against cybercrime and the cooperation between (private and governmental; national and inter- national) parties against cybercrime. What works and why? Do law enforcement agencies use their special powers for crime fighting in a digital world and, if so, with what result? The aim of research into the cybercrime area, is to design crime prevention strategies and measures to effectively disturb/block criminal activities.

6. Risk Management, Economics, and Regulation

Risk management aims to assess the economic value of security, to provide a rational basis for allocating resources to improve security after identifying and assessing risks – and to determine if we are doing enough, or too much, and if we are spending resources on the right things. One central problem here is that concrete data is often lacking, and more research could provide a more solid basis.
A much more fundamental problem is that risk assessment is typically done by an individual party, one of the many parties that collectively provide a complex value chain. For an individual party in such complex value chain there may not be any economics incentives to fix a problem. Indeed, in cyber security there are many externalities : costs that borne by other parties and hence not incorporated in price. For example, someone whose home PC is part of a botnet might not notice any adverse effects, and hence not be motivated to go through all the hassle of cleaning it. Perverse incentives may be a more important cause of security problems rather than the lack of a suitable technical protection mechanisms. A better understanding of the economics of security – and the economic (dis)incentives that occur – is needed for more structural solutions of security problems. Understanding economic drivers – and where these fail – is also crucial to determine where regulation is needed, and more generally what the government's role should be in cyber security. Different regulatory frameworks may apply in the various application domains, and at different levels: national, EU, and international.

7. Secure Design, Tooling, and Engineering

Security engineering is a relatively new field and still lacks the methods and tools to design, build and cost-effectively test secure systems. ICT systems in use today are typically not designed and

built with security in mind. As a result, security is often dealt with retrospectively, only after security problems arise. Security problems then have to be solved by an add-on in the design, when bad initial design decisions can no longer be reversed. When it comes to the software, fixing the problems requires costly bug fixes to patch implementations.
Ideally, systems should be designed with security and privacy in mind from the start – ensuring **Security by Design** or **Privacy by Design**. They should then be implemented and tested using good engineering principles and analysis techniques to avoid security problems or detect them at an early stage. While considerable progress has been made in some niche areas, such as security protocol analysis, sound engineering methods for security are still a long way off, especially when it comes to providing secure software.
Besides software engineering, the field of economics plays an important role in this area. The cost of a secure design may be initially higher and requires a trade-off between risks and expenses. In addition, the cost over time for a secure design is likely to be quite different from that of less secure systems.

8. Operational Cyber-capacities.
Effective and secure ICT, in the form of hardware, software, and networks, is crucial for traditional national defense that relies on ICT. Moreover, cyber-space itself has also become a new domain in which international conflicts play. All this means that cyber operations – operations that target ICT systems or defend against these – are becoming more important, for defensive, offensive, and intelligence gathering capabilities. This straddles themes 2. Malware and 7. Secure Design & Engineering above, but also involves themes 3. Forensics. and 4. Data & Policy Management.

Even if initially aimed at one specific application domain, research on the topics above can provide generic solutions that apply to other application domains. For this to happen it is important that **NCSR A**genda helps to disseminate knowledge and project results across different application domains.

Published by:
Netherlands Organisation
for Scientific Research

Visitor's address:
Laan van Nieuw Oost-Indië 300
2593 CE The Hague

juli 2012

Netherlands Organisation for Scientific Research