Radboud Universiteit

Assessment Report

Computer Science 2015 - 2020

April 2022

Table of contents

RESEARCH REVIEW

Computer Science

2015-2020

De Onderzoekerij
Vondellaan 58
2332 AH Leiden

Phone: +31 6 24812176
Email: info@onderzoekerij.nl
Internet: www.onderzoekerij.nl

Preface

Computer science research, and the products of computer science research, Information and Communication Technologies (ICT), permeate every aspect of our life and our society. ICT has improved our lives considerably, but also the negative side is becoming more and more clear, with some aspects of ICT like social media platforms being divisive and polarising, huge pressure on our energy infrastructure as data centres grow more widespread and demanding, more and more traits of a surveillance society, cyberattacks and even cyber warfare. In academia, all sciences need more and more ICT-specialists, and more and more computer science methods and innovations.

Europe is dependent on big tech companies from the United States and from China, and needs to establish digital autonomy, and needs to step up its digital defense. In the Netherlands, our vital ICT-related companies (such as ASML) need more and more ICT-specialists, educated at the universities and by computer science researchers whose outputs are the subject of this assessment. These researchers are inspired by current applications, and work to achieve the applications and innovations of computer science for the future.

This assessment of the quality of computer science research of most of the Dutch universities was a challenging, but also a very interesting task. Many people, staff members and PhD candidates of computer science departments, staff members and PhD candidates of national research schools as well as the members of the committee, and the secretaries of the committee have worked hard to perform this assessment of computer science research in the Netherlands over the period 2015 - 2020. I sincerely thank everyone involved in this difficult task for their dedication as well as for the pleasant and informative interactions during the site visits, which due to the corona pandemic had to take place entirely online.

The result of all this work is presented in this report. I am very pleased that the main conclusion of the review committee is that computer science research in the Netherlands is of a very high quality, broad and with high impact in international perspective. The committee was pleased to note a lot of collaboration on a national level, and also a start of coordination on a national level (due to the sector plan). We have identified research of top quality in several places. To all departments, we offer a number of constructive recommendations, to motivate them to do even better.

All departments in this assessment have experienced a period of growth in the assessment period. This was very challenging. The committee feels that further growth is indicated for the coming period.

Jos Baeten, Chair of the committee

1. Introduction

1.1 Terms of reference for the assessment

The quality assessment of research of Computer Science is carried out in the context of the Standard Evaluation Protocol For Public Research Organisations by the Association of Universities in The Netherlands (VSNU), the Netherlands Organisation for Scientific Research (NWO), and the Royal Netherlands Academy of Arts and Sciences (KNAW).

The committee was asked to assess the scientific quality and the relevance and utility to society of the research conducted by nine research institutes and three research schools in the reference period 2015-2020, as well as its strategic targets and the extent to which it is equipped to achieve them.

The research institutes are:

- Subdepartment of Computer Science, Eindhoven University of Technology (TU/e);
- Department of Computer Science and Department of Information Science, Open University (OU);
- The Leiden Institute of Advanced Computer Science (LIACS), Leiden University (UL);
- Department of Data Science and Knowledge Engineering, Maastricht University (UM);
- Institute for Computing and Information Sciences, Radboud University (RU);
- Department of Computer Science, University of Twente (UT);
- Informatics Institute, University of Amsterdam (UvA);
- Department of Computer Science, VU University Amsterdam (VU);
- Utrecht Research Institute of Information and Computing Sciences, Utrecht University (UU).

The research schools are:

- Advanced School for Computing and Imaging (ASCI);
- Institute for Programming research and Algorithmics (IPA);
- Netherlands Research School for Information and Knowledge Systems (SIKS).

Accordingly, three main criteria are considered in the assessment: research quality, relevance to society, and viability. During the evaluation of these criteria, the committee was asked to incorporate four specific aspects: Open science, PhD policy and training, academic culture, and human resources policy.

This report describes findings, conclusions, and recommendations of this external assessment of the research of Computer Science.

1.2 The committee

The Board of the participating universities appointed the following members of the committee for the research review:

- Prof. Jos Baeten, Centrum Wiskunde en Informatica (chair);
- Dr. Christine Morin, Inria Rennes (National Institute in Digital Science and Technology), France;
- Prof. Ann Nowé, Vrije Universiteit Brussel, Belgium;
- Prof. Paola Inverardi, University of L'Aquila, Italy;
- Prof. Karl Bringmann, Saarland University and Max Planck Institute for Informatics, Germany;
- Prof. Laurie Williams, North Carolina State university, USA;
- Prof. Alan Smeaton, Dublin City University, Ireland;

- Prof. Eero Hyvönen, Aalto University, Finland;
- Tim Gubner MSc, Centrum Wiskunde en Informatica (PhD candidate).

The Board of the participating universities appointed dr. Annemarie Venemans and drs. Esther Poort of De Onderzoekerij as the committee secretaries. All members of the committee signed a declaration and disclosure form to ensure that the committee members made their judgements without bias, personal preference or personal interest, and that the judgment was made without undue influence from the institutes or stakeholders.

1.3 Procedures followed by the committee

Prior to the site visit, the committee reviewed detailed documentation comprising the self-assessment report of the institute including appendices.

The committee proceeded according to the Strategy Evaluation Protocol (SEP) 2021 - 2027. The assessment was based on the documentation provided by the institute and the interviews with their respective management, selections of senior and junior researchers, and PhD candidate representatives. The interviews took place between January 24 and January 28, 2022 (see Appendix A).

The committee discussed its assessment of each institute during several sessions of the site visit. The committee chair had the coordinating role in the writing procedure and delegated the writing of sections to members of the committee. The members of the committee commented by email on the draft report. The draft version was then presented to the institutes for factual corrections and comments. Subsequently, the text was finalised and presented to the Boards of the universities.

2. General remarks

2.1 Changes in Computer Science landscape

Since the last research assessment in Computer Science six years ago, computer science in the Netherlands has gone through an enormous change. First of all, the number of bachelor and master students in computer science and related fields, such as data science and artificial intelligence (AI) has grown tremendously. Given the situation in the job market, this upward trend is likely to continue. As a result of the increasing student numbers, the research units of this assessment have started to grow. Reinforced by the sector plan, some of the research units have even doubled in size. Coupled with the pull on the best researchers from other countries offering better labour conditions and from big tech companies, this has posed a huge challenge to the Dutch computer science departments.

Also, there have been rapid changes in the field of computer science itself. The combination of data science and artificial intelligence has enabled breakthrough applications, and the area of computer security has grown tremendously. Quantum computing is a growing new field. This required all departments to reconsider their research portfolio.

Computer science is playing an increasing role in many interdisciplinary collaborations (e.g., in the National Research Agenda), leading to new questions and new developments in computer science research itself.

2.2 Status of Computer Science

The committee is happy to see that the research units have met these challenges very well. Research in the units that have been assessed, is in good shape, with many excellent examples of research output and many internationally prominent researchers. Computer science in the Netherlands has always had a strong position with high quality researchers and high international impact. The committee is happy to note that this is still the case.

In the assessment period, funding from national gas proceeds was no longer available, and funding for EIT Digital is declining. However, other forms of funding have become available. Computer science is doing very well in Gravitation funding and is also present in funding from the National Research Agenda. Direct funding from industry has exploded with the start of the ICAI labs, initiated by the Amsterdam Universities but now present on a national scale.

The organisation of the field has improved, with IPN playing an important role, with its Special Interest Groups and role in the sector plan.

2.3 Needs of Computer Science

In this general section, the committee first wants to address two important issues that need improvement. First of all, funding opportunities for core computer science need to improve. Second, the research staff (especially junior staff) need more time for research.

The first major issue is that the funding landscape in the Netherlands is heavily skewed towards application-oriented and multidisciplinary research, to the detriment of research in core computer science. This point is also made very well in the IPN Vision document (https://ict-research.nl/wordpress/wp-content/uploads/2022/01/IPN-vision-paper-ENG.pdf). This situation is not satisfactory, because future innovations and applications will arise from research in core computer science.

The units involved in this assessment have succeeded in filling many new staff positions in recent years, in many cases by offering starting packages to incoming junior staff. For the retention of these staff members, it is essential that they can find and grow their research specialisation by means of personal grants. For this, they rely on the personal grant competitions of NWO and ERC. Dutch computer scientists do well in the ERC competition, but the success rates at NWO are far too low, given the size and importance of the field. One reason for this is the use of evaluation panels not composed of computer science experts only. The committee recommends that NWO sets aside adequate funding for computer science in the personal grant schemes VENI, VIDI, VICI, improving the success rates to 30% at least.

The second major issue is that the research units have grown in size in this review period, but that student numbers have increased at an even higher rate, resulting in a high student-staff ratio. Given the situation in the job market, it is not likely that this trend will be reversed in the near future. Therefore, it is imperative that first-stream funding for computer science increases. The best way to achieve this is to have another Sectorplan for computer science. The added benefit of such an additional Sectorplan is that the coordination in the sector improves. This time, the Sectorplan should include all ordinary members of IPN.

2.4 Research quality

Despite the huge challenges the departments have faced in the assessment period, the research units have met these challenges and maintained (in some cases improved) their research quality and international standing and collaboration.

Because of the change in evaluation procedures in the new SEP protocol 2021-2027, some research metrics can no longer be used in the evaluation. However, all research units exhibit examples of research output with very high impact, and present important marks of recognition. The committee recommends developing other research metrics (with fewer drawbacks as the current ones) to supplement the more narrative self-assessments of the current assessment. For instance, each research institute could mention the top venues where they want to publish, and then give the number of times they succeeded in doing so.

2.5 Societal relevance

All research units in the assessment have many examples of research programmes with high societal relevance and also perform well in outreach activities. There are ample funding possibilities for large programmes with high societal relevance in the short term. For innovations and applications in the longer term, it is necessary to strengthen core computer science research.

The Innovation Centers in Artificial Intelligence (ICAI labs) have increased direct funding from industry and other organisations considerably.

Some units employ internally funded research software engineers to sustain the impact of research collaborations with industry and other organisations. The committee feels this is a welcome development, as it increases software output quality, visibility, and impact.

2.6 Viability

The viability of the sector is very good. However, as mentioned before, there are two major concerns. First, the funding possibilities for the departments are limited. All units have gone through a period of

growth and attracted many new staff members in a very competitive job market. For the retention of this incoming staff, and further growth of the units, it is essential that the funding possibilities in core computer science improve. The success rate of computer science proposals in the personal grant scheme of NWO should be at least 30%. The committee is pleased to note that many units offer starting packages to incoming junior staff, such as an internally funded PhD student. The committee recommends that units without these packages also consider this.

The other major concern is that the student-staff ratio in the units is still far too high. The committee recommends that there is a second Sectorplan for computer science, involving all ordinary members of IPN, to improve this balance and further coordination between the units.

2.7 PhD programme

The units in the assessment all have a well-thought-out PhD programme. With these programmes, the units produce excellent researchers that are internationally competitive. Issues are drop-out rate and time taken to completion, which are too high in some units. Some units are recommended to employ a stricter Training and Supervision Plan, with some mandatory courses, making this less dependent on the supervisor. An interesting introduction is the TA-PhD, with a longer completion time and a higher teaching load. This seems to work well, but needs to be closely monitored.

2.8 Open science

The units have addressed the challenges of open science with various degrees of success. Some units need to work at divulging open science practices to all members of staff and PhD candidates. Some units have already taken measures for proper management of research data (FAIR, GDPR, etc). Some units stand at the forefront, others need to push forward the efforts to ensure all staff are well trained to write data management plans.

For open access, Dutch universities are spending an enormous amount of money in transformative agreements with large commercial publishers. This is not an effective way of spending public money to further open science. A lot more can be achieved, if this money is used directly on diamond journals and proceedings, or gold journals and proceedings with low article processing charges (APCs).

2.9 Working environment and personnel policies

Concerning the ethics of computer science, all units are aware of possible misuse of products of computer science research, and of the risks of collaborating with research partners with dubious ethical practices. Still, the committee feels that the role of ethical review boards needs to be enhanced, in any case in contract negotiations, more in general in all projects, and that there needs to be more computer science expertise in these review boards.

Further, the committee feels that in some cases, academic freedom is limited. There should always be some room for curiosity-driven, blue-sky research, as it will open unexpected applications.

A welcome development since the previous assessment is that currently, associate professors can have the ius promovendi (in some units, under some conditions), that is the right to promote students to a doctorate. This gives them greater independence and visibility through their own PhD candidates.

The committee has the impression that there is strong awareness of and ample examples of proactive action regarding diversity in terms of nationality and gender. However, in all units, representation of women at all levels is still too low. Communication between the units is encouraged to adopt best

practices. Other aspects of diversity, such as people with disabilities, migration background or ethnicity, get far less attention.

An explicit strategy regarding the support for diversity in all its aspects appears to be lacking in some of the units. The committee recommends that the institutes continue to build increased awareness of diversity in many aspects in order to promote the establishment of a more balanced structure at all levels.

The committee sees differences within the units in the amount of time staff spend on research and education. In the framework of the Recognitions and Rewards programme, this can also work well. The committee warns against creating staff positions devoted only to teaching, as academic teaching needs to have a strong connection to research. The units are encouraged to improve student-staff ratios by other means.

The units realise that the work pressure on incoming staff and tenure track staff is high. The amount of support the units offer varies. In general, the units should consider what kind of support they offer to help junior staff with open science, proposal writing, project management, data management plans and so on.

2.10 Conclusion and recommendations

Computer science in the Netherlands has always had a strong position with high quality researchers and high international impact. The committee is happy to note that this is still the case.

Despite the huge challenges the departments have faced in the assessment period, with a tremendous increase in student numbers and a brain drain to big tech companies and other European countries such as Germany and Switzerland, the departments have met these challenges and maintained (in some cases improved) their research quality and international standing and collaboration.

The committee makes the following recommendations for further improvements in the future:

- More funding for core computer science is needed. For instance, success rates for computer scientists in the personal grant funding from NWO needs to rise to more than 30%;
- A second Sectorplan for computer science is needed to improve the student-staff ratio in computer science and to increase coordination between the members of IPN;
- The committee recommends to make room for curiosity-driven, blue-sky research;
- The committee recommends developing other research metrics (with fewer drawbacks as the current ones) to supplement the more narrative self-assessments of the current assessment;
- The use of research software engineers to increase the impact of research is a welcome development;
- The committee recommends that all units provide starting packages to incoming junior staff;
- Dutch universities spend too much money on transformative agreements with large commercial publishers. It is much more effective to spend this money on open science initiatives directly;
- The use of ethical review boards needs to be enhanced;
- The units are encouraged to pay more attention to diversity, in all its aspects.

7. Institute for Computing and Information Sciences, Radboud University

7.1 Organisation, strategy and targets

The Institute for Computing and Information Sciences (iCIS) is a medium-sized department of the Faculty of Science of the Radboud University (RU). The department has experienced in the current assessment period a fifty per cent growth in the scientific staff (31/45) and a moderate growth in postdocs and PhD candidates (74/82).

The institute is divided into three sections. Each section focuses on a research theme: the *software* theme in the Software Science Section, the *data science and artificial intelligence* theme (subfields *data modeling & analysis* and *machine learning*) in the Data Science Section, and the *security and privacy* theme in the Digital Security Section.

The research mission of iCIS is to improve the security, reliability and validity of computer systems and algorithms through mathematically founded theories, methods, and tools.

The institute considers pure curiosity-driven research as crucial to fertilise the research landscape to foster future applied research. Research problems are inspired by concrete problems stemming from reality and by investigating limits and theoretical assumptions of computer science and their potential impact for developers and system integrators.

7.2 Research quality

The iCIS department has a consolidated structure in the three areas of interest. Each section has flagship research themes that are internationally recognised. A limited number of new research areas have been introduced to complement/modernise the core areas focus. This broadening of topics goes in small steps due to the moderate increase of staff and the strategic choice to maintain the international standing of the core areas.

The overall quality is very high in terms of publication venues, scientific value, awards, and individual grants. The unit has a tradition and a policy, maintained in the assessment period, in delivering open-source research software artifacts that are successfully transferred in the academic, industrial, and societal communities of their eco-system generating direct and indirect impact. Collaboration with the eco-system actors is also strengthened through a set of nationally funded collaborative projects and ICAI (Innovation Centre for Artificial Intelligence) labs.

Publications of iCIS researchers have generated multiple follow-ups in terms of industrial and scientific interest. The researchers are also very active in the international community in promoting benchmarking activities, participating, and organising international competitions, participating in international networks and standardisation bodies. There is clear evidence that they actively participate in their respective international research communities through multiple activities, like the Automata Wiki initiative, the participation in cryptography standardisation initiatives, and the ELLIS unit.

During the assessment period, iCIS researchers have been able to attract 3 ERC advanced grants, 1 ERC starting grant, a VIDI, a VENI and a Marie Sklodowska-Curie fellowship. Although this is a very good record, the figures provided in the self-assessment show that there has been an absolute and relative decrease of funding in research grants in the past six years. This data suggests that beyond the

remarkable performance of some researchers, the overall performance of the iCIS researchers in obtaining funding in the reference period 2015-2020 is not on a positive trend. The same trend is also visible in the acquiring of contract research, measuring the ability of the department to productively interact with the industrial actors of their eco-system.

Despite its scientific international visibility, the unit seems to not consider developing international collaboration through Horizon projects as a priority. The committee understood from the interviews that the institute rather focuses on personal grants, and has been able to achieve a higher-than-average success rate because of its selective approach. Although the unit has initiated training events, and has organised with Radboud Innovation to share a monthly newsletter that reviews upcoming international collaborative calls, the committee is of the opinion that the unit should have put in place measures that can help the applicants in terms of administrative burden and difficulties in writing and shaping a proposal rather than just advertising calls. The committee encourages the management to explore ways to acquire international funding.

iCIS has recently launched the Innovation fund for blue-sky research that aims to offer to any member of the staff, on a five-year period, the possibility to have a PhD funded internally. This is a positive initiative that may help involve a larger number of staff in active research.

7.3 Societal relevance

The institute has a good network to link to society. Primarily it exploits the initiatives carried out at the university level that facilitate inter university and intra society collaborations. Some research themes, for example in the data science, privacy and security domain, have a higher readiness level than other themes for the society at large. However, significant overall effort in bringing scientific discoveries to societal values through different levels of personal engagements and relationships with the economic side of the society (both public and private) has been observed. For example, the committee appreciates the new open-source graph database system that combines methods from databases and information retrieval for ranking property graphs to counter Big Tech's dominance in search and social media.

It is worth noticing the bunch of activities carried on the educational side that move in the direction of innovating teaching in different areas of computer science. This is an extremely important although not easily rewarded innovation area that can help mitigating the lack of ICT-skills the society is suffering.

Connections to industry through PhDs remain the most practiced way to achieve individual researcher collaborations with IT industries and other IT bodies, complemented with internships at the bachelor and master level. This seems an area where a more structured approach would make impact more visible.

7.4 Viability

The institute's strategy for the next years will keep investigating the three research themes with the same research methodology: on one hand pursuing curiosity-driven research that may anticipate solutions for new emerging ICT developments, on the other hand exploiting knowledge transfer back and forth from society and industry for the formulation of research questions and application of research results.

The institute has a number of strengths as detailed in their SWOT analysis, notably their flat and open management structure, the presence of leading scientists, and the possibility of blue-sky research

through the internal Innovation fund. The SWOT analysis also identifies weaknesses that require further specific attention. The first weakness concerns funding: the need to increase the number of researchers that can acquire grants and thus expand their research, the different capacity of the sections to attract funding, and the modest involvement of the institute in European collaborative projects. The committee has learned from the interviews that iCIS has a very good success rate in the NWO competitive calls. Furthermore, iCIS supports researchers in the choice of calls depending on the level and maturity of their research. However, this policy seems mainly directed to individual grants and to excellent researchers. Collaborative projects, especially European ones, may be too constrained and require strong links with industrial/public partners and a strong international network. Competent support, for example training events, can help but is currently not sufficient. Explicit policies to reward the researchers that engage in competitive applications may be useful. For example, researchers may be promised a small funding if a project is not funded but has reached a certain threshold.

The other proposed countermeasures may not hit the target. Indeed, pushing for external contracts by strengthening the links with industrial partners and/or the hospital, as well as promoting cross-section research can be beneficial for the institute but may not help individual researchers in expanding their research.

Finally, the weaknesses concerning the risk of missing relevant research topics because of too focused research remains unconfronted. Indeed, the previous research assessment recommended *"… that iCIS continues focusing on publishing in high quality venues and growing new research areas based on interactions with new areas and disciplines, in addition to maintaining their standards of excellence in their core areas of computer science."* The exploration for new research area to grow has been limited. In the opinion of the committee, the institute has a solid core base, and it is in the position to accept a moderate risk and to explore new research themes in the sections and beyond the section's themes. The foreseen recruitment plan could be exploited to acquire expertise that is not present now but might become crucial in the future. The faculty's strategy to create the interdisciplinary research platform can be the context in which some of these initiatives can be developed.

7.5 PhD policy and programme

At RU the educational and training requirements of doctoral candidates are formalised in a Training and Supervision Plan (TSP). The TSP is custom tailored to each PhD candidate's needs. RU has two mandatory courses: 'Didactical Skills' and 'Scientific Integrity'. However, PhD candidates typically have teaching duties (roughly 10% of their time). The committee recommends that the TSP should be made more explicit and less reliant on the individual supervisor(s). For instance, RU should consider adding mandatory courses for transferable skills and good practices (Scientific Integrity, writing, presentation).

In their TSP, PhD candidates typically follow courses offered by Research schools IPA and SIKS, as well as generic courses offered by RU. From conversations, it appeared that courses on didactic training lacked a hands-on component. In addition, the committee recommends introducing a course on writing grant proposals as such a course would clearly benefit PhD candidates as well as junior staff.

Most PhD candidates have two supervisors. In exceptional cases, however, some PhD candidates who started before September 2020 only appear to have their promoter as their sole supervisor. PhD candidates tend to have regular, mostly weekly meetings, with their supervisors as well as meetings on a "on need" basis. Yearly, the PhD candidate's performance is evaluated, plans for the next period are made and, if needed, the TSP is updated. After the first 12 months, a go/no-go decision is made whether the PhD track should be continued.

At RU, it is common that PhD candidates spend some time abroad. The committee agrees that this can help PhD candidates to extend their network and prepare them for future jobs. In addition, PhD candidates receive job guidance from their supervisor as well as from a university-wide job fair. The job fair, however, appears to have been postponed due to COVID.

The committee commends that, at RU, there are virtually zero dropouts (4%). But, only a quarter (25%) of PhD candidates graduate within 4 years and 3 months and roughly half completed their PhD within 5 years. It is noteworthy that RU has introduced a monetary incentive for PhD candidates to graduate in time.

7.6 Open science

According to the committee, iCIS has been at the forefront of promoting open science practices in the university. The institute adopts the policy to release open-source research software. It also pushes for open access publications. In this direction it has volunteered as first institute at RU to participate in a pilot project to make all the short scientific works available in open access via the Radboud Repository.

The institute has contributed to the development of the university research data management plan and has written its own RDM policy. It has made efforts to improve findability and accessibility of research data that resulted in an increased number of registered and deposited data sets. Active involvement of scientists, early career researchers and PhD is stimulated to drive the change.

7.7 Working environment and personnel policies

7.7.1 Academic culture

From the self-evaluation report and from the interviews with junior staff and PhDs, emerges the view of a working environment that cares for its members in multiple dimensions. The department has put in place formal and informal policies to ensure openness, safety, and inclusivity. Because of the flat organisation, the institute has short communication lines. English is the main language for research and teaching staff meetings.

7.7.2 Human resources policy

The institute targets the recruitment of excellent talents. In the last years, it has doubled the number of assistant professors and increased the number of full professors with 50%. Recruitment has also targeted diversity in terms of gender and nationalities, and it has succeeded in improving the respective percentages. Future plans will keep on the same objective, especially in the units that still suffer of severe gender unbalance.

Gender diversity is a top priority of the institute's agenda. In 2017, the institute won the second Minerva Informatics Equality Award in recognition for its measurable efforts in monitoring gender issues and promoting the advancement of female careers in Informatics. The Radboud Women of Computing Science (RWoCS) organises events to connect women, both students and employees, who are studying or working in Computing Science or related fields. The committee appreciates these efforts and urges the institute to continue this.

The career path for young researchers is well defined and communicated transparently at the beginning of the employment. Despite the general focus of the Institute on excellence, there is an effort to not put

pressure on young researchers in terms of publication criteria for promotion. Indeed, from the interview with junior staff, the general feeling was that promotion is the result of an overall evaluation and that there is no need and pressure to excel in all criteria.

The committee is positive about the specific role of a tenure track counsellor, covered by a senior scientist, that has been created to support tenure track researchers.

7.8 Conclusions and recommendations

7.8.1 Conclusion

iCIS is a medium size department with a well-defined research profile. It covers three macro-themes: Software, Data-Science and Security. Within each theme there are specific core research areas that excel at the international level. This is demonstrated by the awards, competitive grants, impactful research software and visibility in the international community through invited talks and committee participations. The department has a strong network of contacts to the society, and it is well positioned to embark on interdisciplinary research through the university and faculty initiatives. iCIS demonstrates active attention to maintaining high quality of the working environment, favouring openness, inclusivity, transparency, and reliability especially for younger researchers and PhDs.

Research-wise iCIS is a top player in its field of expertise and is highly motivated in maintaining this position. However, in the opinion of the committee, this is at the expense of being too conservative. New research topics are added incrementally to the core ones, application of the core expertise in different domains and cross-sections is ranked first in iCIS strategy for the future. Although the institute introduced a blue-sky research fund, a limited plan or strategy to open new core areas or significantly widen the existing ones is foreseen.

The committee feels that in the present fast-changing ICT landscape with iCIS entering a five-year period that may see a significant turnover due to retirements coupled with the availability of extra funding, a long-term view of where iCIS would like to be in five to ten years' time is crucial, in order to steer the next development phase. The committee recalls here that the mission of iCIS is to improve security, reliability and validity of computer systems and algorithms through mathematically founded theories, methods and tools. Computer systems and algorithms are changing dramatically in the future, in their architecture, software, computational models and more. In order to maintain its mission and leadership, iCIS needs to start considering some of these changes.

7.8.2 Recommendations

The committee makes the following recommendations for further improvements:

- The committee recommends that iCIS continues focusing on its core area of expertise but at the same time engages in the effort to develop a longer-term strategy that may suggest new research areas to invest in. A long-term view where iCIS would like to be in five to ten years' time is also crucial to steer the next development phase;
- The committee encourages iCIS to accept a moderate risk and to explore new research themes in the sections and beyond the section's themes. The foreseen recruitment should also focus on acquiring expertise that is not present now but might become crucial in the future;
- The committee encourages the management to explore ways to acquire international funding;

- The management should encourage participation in European collaborative projects. This is not only useful to improve research funding but also to expose researchers to different research and industrial priorities and cultures;
- Interdisciplinarity is increasingly important as ICT is the enabler of the digital society. The committee recommends that iCIS members engage in inter-disciplinary projects, but maintaining a CS foundational approach, mitigating the risk of CS as a service approach;
- The committee recommends a more structured approach to make the impact by individual researcher collaborations with IT industries and other IT bodies more visible;
- The committee advises to make the TSP more explicit and less reliant on the individual supervisor, for instance by adding mandatory courses for transferable skills and good practices (Scientific Integrity, writing, presentation).

Appendix A - Programme of the visit

Sunday January 23

Time	Part
16.30 - 18.00	Committee meeting

Monday January 24

Time	Part
08.30 - 09.00	preparation programme TU/e
09.00 - 09.45	management
09.45 - 10.00	break
10.00- 10.30	PhD candidates
10.30 - 11.05	senior staff
11.05 - 11.15	break
11.15 - 11.50	junior staff
11.50 - 12.15	preparing questions for 2nd meeting management
12.15 - 12.35	2nd meeting management (additional questions)
12.35 - 13.45	lunch and reflecting programme TU/e
14.00 - 14.30	preparation programme OU
14.30 - 15.15	management
15.15 - 15.30	break
15.30 - 16.00	PhD candidates
16.00 - 16.35	senior staff
16.35 - 16.45	break
16.45 - 17.20	junior staff
17.20 - 17.45	preparing questions for 2nd meeting management
17.45 - 18.05	2nd meeting management (additional questions)
18.05 - 18.30	reflecting programme OU

Tuesday January 25

Time	Part
08.30 - 09.00	preparation programme UL
09.00 - 09.45	management
09.45 - 10.00	break
10.00- 10.30	PhD candidates
10.30 - 11.05	senior staff
11.05 - 11.15	break
11.15 - 11.50	junior staff
11.50 - 12.15	preparing questions for 2nd meeting management

12.15 - 12.35	2nd meeting management (additional questions)
12.35 - 13.45	lunch and reflecting programme UL
14.00 - 14.30	preparation programme UM
14.30 - 15.15	management
15.15 - 15.30	break
15.30 - 16.00	PhD candidates
16.00 - 16.35	senior staff
16.35 - 16.45	break
16.45 - 17.20	junior staff
17.20 - 17.45	preparing questions for 2nd meeting management
17.45 - 18.05	2nd meeting management (additional questions)
18.05 - 18.30	reflecting programme UM

Wednesday January 26

Time	Part
08.30 - 09.00	preparation programme RU
09.00 - 09.45	management
09.45 - 10.00	break
10.00- 10.30	PhD candidates
10.30 - 11.05	senior staff
11.05 - 11.15	break
11.15 - 11.50	junior staff
11.50 - 12.15	preparing questions for 2nd meeting management
12.15 - 12.35	2nd meeting management (additional questions)
12.35 - 13.45	lunch and reflecting programme RU
14.00 - 14.30	preparation programme UT
14.30 - 15.15	management
15.15 - 15.30	break
15.30 - 16.00	PhD candidates
16.00 - 16.35	senior staff
16.35 - 16.45	break
16.45 - 17.20	junior staff
17.20 - 17.45	preparing questions for 2nd meeting management
17.45 - 18.05	2nd meeting management (additional questions)
18.05 - 18.30	reflecting programme UT

Thursday January 27

Time	Part
08.30 - 09.00	preparation programme UvA
09.00 - 09.45	management
09.45 - 10.00	break

10.00- 10.30	PhD candidates
10.30 - 11.05	senior staff
11.05 - 11.15	break
11.15 - 11.50	junior staff
11.50 - 12.15	preparing questions for 2nd meeting management
12.15 - 12.35	2nd meeting management (additional questions)
12.35 - 13.45	lunch and reflecting programme UvA
14.00 - 14.30	preparation programme VU
14.30 - 15.15	management
15.15 - 15.30	break
15.30 - 16.00	PhD candidates
16.00 - 16.35	senior staff
16.35 - 16.45	break
16.45 - 17.20	junior staff
17.20 - 17.45	preparing questions for 2nd meeting management
17.45 - 18.05	2nd meeting management (additional questions)
18.05 - 18.30	reflecting programme VU

Friday January 28

Time	Part
08.30 - 09.00	preparation programme UU
09.00 - 09.45	management
09.45 - 10.00	break
10.00- 10.30	PhD candidates
10.30 - 11.05	senior staff
11.05 - 11.15	break
11.15 - 11.50	junior staff
11.50 - 12.15	preparing questions for 2nd meeting management
12.15 - 12.35	2nd meeting management (additional questions)
12.35 - 13.45	lunch and reflecting programme UU
14:00 - 14:30	ASCI (staff and PhD's)
14:40 - 15:10	IPA (staff and PhD's)
15:20 - 15:50	SIKS (Staff and PhD's)

Appendix B- Quantitative data

Institute for Computing and Information Sciences, Radboud University

Table 5.1 Research staff in # and fte – RU

	2015		2016		2017		2018		2019		2020	
	#	fte	#	fte	#	fte	#	fte	#	fte	#	fte
full prof	12	7.7	14	9.2	16	11.1	16	10.8	17	10.0	17	11.1
associate prof	8	5.6	8	4.4	6	2.4	5	2.3	5	2.9	6	2.4
assistant prof	11	9.7	13	10.9	15	12.8	16	15.6	19	13.9	22	17.9
all prof	**31**	**23**	**35**	**24.5**	**37**	**26.3**	**37**	**28.7**	**41**	**26.8**	**45**	**31.4**
PD	30	18.7	26	14.3	22	16.1	25	12.0	21	10.6	18	8.0
PhD	44	34.2	46	36.8	43	35.2	39	28.9	52	33.0	64	40.6
all PD + PhD	**74**	**52.9**	**72**	**51.1**	**65**	**51.3**	**64**	**40.9**	73	**43.6**	**82**	**48.6**

Table 5.2 Funding – RU

	2015		2016		2017		2018		2019		2020	
Funding in M€/%	*M€*	*%*	*M€*	*%*	*M€*	*%*	*M€*	*%*	*M€*	*%*	*M€*	*%*
Direct funding	2.9	43.0	3.6	49.2	3.5	47.6	3.8	50.5	4.4	59.8	5.6	65.7
Research grants	2.0	29.5	2.1	28.3	2.1	28.1	1.6	21.4	1.9	25.3	1.7	20.3
Contract research	1.3	18.8	1.1	14.4	1.1	14.3	0.9	11.9	0.9	11.6	0.8	9.1
Other	0.6	8.7	0.6	8.0	0,7	10.0	1.2	16.2	0.2	3.3	0.4	4.9
Total funding	**6.786**		**7.315**		**7.424**		**7.448**		**7.384**		**8.501**	
Expenditure in M€/%												
Personnel costs	5.9	90.1	6.1	87.1	6.5	88.5	6.7	86.8	6.7	89.8	7.7	93.8
Other costs	0.6	9.9	0.9	12.9	0.8	11.5	1.0	13.2	0.8	10.2	0.5	6.2
Total expenditure	**6.508**		**7.045**		**7.353**		**7.707**		**7.432**		**8.218**	

Table 5.3 PhD completion – RU

Enrolment				**Cumulative success rates**											
Starting year				≤ 4 yr + 3 mo		≤ 5 yr		≤6 yr		Until Dec 2020		Ongoing		Discontinued	
	M	F	M+F	#	%	#	%	#	%	#	%	#	%	#	%
2012	2	2	4	1	25	2	75	0	75	0	75	1	25	0	
2013	12	1	13	3	23	3	46	6	92	0	92	1	8	0	
2014	3	1	4	0	0	2	50	1	75	1	100	0	0	0	
2015	14	2	16	4	25	4	50	0	50			6	38	2	
2016	8	0	8	2	25	1	38					5	62	0	
2017	3	0	3									3	100	0	
2018	6	1	7									7	100	0	
2019	15	4	19									19	100	0	
2020	16	7	23									23	100	0	
Total	79	19	98	**10**		**12**		**7**		**1**		**65**		**2**	

Radboud University

iCIS Response to the

Research Assessment Report

Research Assessment Computer Science, 2015-2020

Response to the research assessment report

We thank the committee for the time and effort dedicated to evaluating 9 institutes (including iCIS) and 3 research schools, and providing us with a well-balanced review report on Computer Science in The Netherlands. We appreciate the positive assessment of scientific quality, societal relevance and viability of our research, and were pleased to read that the committee could recognise our efforts to create an academic culture that provides a working environment that cares for its members.

The committee has made a number of concrete suggestions at the institute and the national level, which we address below.

Institute

Develop a longer-term strategy, explore new research themes beyond the sections' themes. The committee report suggests a top-down organised, long-term strategy underpinning the five to ten year research horizon.

While recognizing the value of this approach, we have to face the situation on the job market for computer science in The Netherlands: few people with PhD degrees pursuing a career in academia, high salaries in industry, and high salaries in academia in near-by countries like Germany. Our recruiting strategy therefore has concentrated on attracting young and promising talent to join our institute, and grow our research areas accordingly; leading to a more bottom-up, organic model to discover and develop research areas in which to excel.

Already, this brought us Human-Computer Interaction as an emerging theme that cross-cuts all three sections, a number of (recent) successes in the fast developing area of dependable AI, a new research collaboration in the iHub on "dark patterns", and the creation of a new MSc programme Cybersecurity & AI, starting September 2023.

We would further like to highlight the role served by our “blue-sky research” fund in this context; an excellent instrument to provide our staff the freedom to re-orient their research in response to changes in the field.

We agree with the committee that a mechanism is needed to bring together these two approaches, and prioritise investments in topics for new positions. Both bottom-up "arising" topics and top-down "agenda topics" are therefore discussed at our institute retreats; one scheduled this fall, for example.

Acquire more international funding. We agree with the recommendation to invest in the acquisition of a larger share of (international) collaborative research projects in our project portfolio. We plan to follow-up upon the suggestion to formulate an explicit policy to reward researchers that engage in competitive applications and reach a certain threshold, even if the project is not funded.

Engage in interdisciplinary projects, yet mitigate the risk of CS as a service approach. Our research agenda is driven by the need for pure computer science research. We participate in new and rising topics at the iHub, Radboud AI and the Faculty's initiatives, to demonstrate the usefulness of our methods for other scientific disciplines, but, without losing sight of our main ambition: to improve computer-based systems and algorithms, applicable across a range of applications.

Make the impact by individual researcher collaborations more visible. We will respond to this recommendation with the revision of the institute website, through the university-wide project Klantgericht Online that helps us revise and improve our online presence.

Make the TSP more explicit and less reliant on the individual supervisor. The recently implemented Hora Finita PhD monitoring system and the appointment of associate professor Krebbers as director of our institute's graduate school will aid in the harmonisation of supervision and training practices of

PhD candidates in our institute. All PhD candidates get training in didactics and scientific integrity; we will consider the committee's suggestion to consider the addition of "writing grant proposals".

National

The committee has also made recommendations for computer science in the Netherlands, beyond individual institutes. We highlight two recommendations that are especially relevant in our context:

Make room for curiosity-driven, blue-sky research. We have created the "iCIS Innovation Fund" for blue-sky research to enable every staff member to supervise one PhD candidate on a topic of their choosing, funded directly by the institute, once every five years. We will have to expand this fund proportionally in relation to the expected and continued growth in personnel.

The use of ethical review boards needs to be enhanced. We agree that this is a topic of concern, both with respect to the assessment of the ethical dimensions of the anticipated research itself, as well as the partnerships in which the research is carried out (also related to the topic of "kennis veiligheid"). We need to support our researchers with more guidance toward a complete assessment of all ethical aspects of their projects and plans. The current research director iCIS has joined the university's "Programmagroep Kennisveiligheid", providing active connections to developments in this domain locally and nationally.

Radboud University

Excerpt from the

Self-evaluation report

Research Assessment Computer Science, 2015-2020

Summary of the self-evaluation report

Radboud University's Institute for Computing and Information Sciences (iCIS) is a medium-sized department in the Faculty of Science, on a mission to improve the security, reliability and validity of computer systems and algorithms through mathematically founded theories, methods and tools.

Our research agenda is driven by the need for *pure computer science research;* to develop new paradigms and go beyond knowledge boundaries, to ensure the foundational results needed for industry and open source community to build upon in the future as they do today. The applicability of the institute's methods and tools is validated by tackling problems in society, industry, and other scientific disciplines. Seeing how computing can open up new opportunities for other sciences to understand phenomena in their fields, we invest in demonstrating the usefulness of our methods for other scientific disciplines. But, without losing sight of our main ambition: to improve computer-based systems and algorithms, applicable across a range of applications.

iCIS' activities are concentrated on three themes in the national Sector Plan Beta & Techniek: *software, data science and artificial intelligence*, and *security and privacy.* The increasing awareness of the societal relevance of, dependence on, and potentially harmful effects of ICT opens up new opportunities for funding fundamental research in all three areas. A strategic goal going forward is to strengthen research across themes, especially in AI & security and AI & verification.

We publish the majority of our research in open access, with a focus on high impact conferences and journals because that is the fastest way to reach others with our work. The goal is to make all our short scientific works available in open access via the Radboud Repository (using Article 25fa of the Copyright Act where necessary). As research software leads to research quality *and* societal impact, we encourage staff to release their software, in open source, using liberal licenses. Our research data management policy is written from an open science perspective, the data steward role assigned to a scientist, and we foster active involvement of early career researchers and PhD candidates.

Growth in student numbers and funding has led to a higher budget and new (permanent) staff positions. It also let us establish the iCIS Innovation Fund, that enables every staff member to supervise one PhD candidate on a topic of their choosing, funded directly by the institute, once every five years. A downside of this growth however, is the prolonged high work pressure for our staff, as the costing model causes a lag between increases in workload and expansion of the institute. This situation worsens as attracting and maintaining staff is a challenge due to the labour market: few qualified people, high salaries in industry, and high salaries in academia in near-by countries like Germany. Our hiring strategy focuses on new, young talent, who we aim to recruit early in their career (when compared to other areas in the sciences) and train in-house for higher ranks.

The institute promotes a scientific atmosphere which is open and attractive for all members of the institute. In 2017, we received the Minerva Informatics Equality Award for our efforts in monitoring gender issues and promoting the advancement of female careers in Informatics. Also, we support PhD candidates who want to widen their horizon beyond their research topic, to spend a small part of their PhD project abroad, at another university or research institute, or in industry.

iCIS acts as lead partner in Radboud AI and the Radboud iHub. The institute has close ties to RadboudUMC, TNO, PI.Lab and the embedded systems institute (ESI), excellent contacts and outlets for contract research and valorisation, in industry, government agencies, financial institutions, and utility companies. We plan to respond to Europe's push to Digital Sovereignty to improve our visibility in EU funding networks. While contract research for external partners like Google, Intel and the Dutch Payment Association helps maintain a healthy volume of research, we ensure that external funding never endangers our independence; society relies on academia to perform research that may occasionally be unwelcome to some private parties.

Case studies

We present six case studies to showcase innovative research lines, grown in the assessment period, that have great opportunities for further development in the coming years:

1) Model learning
2) Real-world crypto
3) Causality
4) Machine Learning, Security, and Privacy
5) Radboud iHUB: interfaculty research hub on digitalization and society
6) Building ecosystems for Artificial Intelligence research and applications

The first three case studies highlight one area per Section, directly linked to the three focus topics selected by iCIS in the national Sector plan. The fourth case study crosses the research in two sections, Digital Security and Data Science, and has inspired the plans to create the new MSc specialization AI & Security, anticipated to start September 2022. The fifth case study highlights the Radboud iHub, a unique interdisciplinary initiative sprung out of iCIS, supported by seed funding provided by the Board to enable this research to grow to fruition. The iHub addresses the big challenges to society raised by ICT and brings together research from all Faculties on the campus. The final case study presents how we approach the topic of Artificial Intelligence at Radboud University: from three key angles, computing science at iCIS, neural science at the Faculty of Social Science and the Donders Institute, and health at the academic hospital, creating synergy by bringing these three perspectives together under one umbrella in Radboud AI.

B.1 Model Learning

The mission of the Software Science group is to do top research on the use of models for design and analysis of software, bridging the gap between theory and applications. In this case study, we describe how we realized this mission in the area of active automata learning, a.k.a. model learning, in close collaboration with partners from academia and industry.

Our research in this area was triggered by a practical challenge. Our society has become completely dependent on network and security protocols such as TCP, TLS, SSH, and Wifi. Usually we have formal correctness proofs of high-level versions of these protocols, but finding errors in implementations turns out to be difficult. Due to the size and complexity of the source code it is not possible (or cost effective) to apply existing techniques from program verification or model checking. Nevertheless, finding errors is important as they may lead to security breaches or even complete network failures.

Building on seminal work of Dana Angluin, we explored the use of active automata learning to extract models directly from protocol implementations, followed by model checking to find bugs in the derived models. In collaboration with Bengt Jonsson (Uppsala), we developed a theory of abstractions that allowed us to abstract the complex behavior of network protocols into small Mealy machines that can be learned by state-of-the-art learning tools. In a series of papers, written by members of the SWS and the DiS groups, we showed that model learning is able to find standard violations and bugs in implementations of major network protocols such as TCP, TLS, and SSH, leading to several bug fixes in these implementations. An example of this line of work was presented at CAV'16. We revealed several instances in which TCP implementations (Windows, Linux,..) do not conform to the RFC specifications. In 2018, we organized a Lorentz Center workshop on Systematic Analysis of Security Protocol Implementations. This workshop demonstrated that if you bring together security protocol experts with experts on model learning, it is possible to obtain interesting models in a matter of days.

Triggered by the successes in the area of protocols, the question arose whether model learning could also be used to construct models of legacy software. To deal with the increasing amount of software, Dutch high-tech companies employ component-based software architectures with components that interact via explicitly specified interfaces. For newly developed components these interfaces are specified, for instance, using the ComMA open source tool of which SWS member Jozef Hooman is one of the main developers. However, for legacy components such interfaces are typically not available. In a case study from 2015, we succeeded to learn a model of the Engine Status Manager (ESM), a software component that is used in printers and copiers of Oce/Canon. With Philips Healthcare, we explored the use of model learning to compare a legacy component (a power control service of an X-ray scanner) with its refactored implementation. A presentation about this work at the TNO ESI symposium in April 2016 led to the Transposition project from ASML and TNO ESI, in which model learning is used to obtain interface models of ASML TWINSCAN software components. Together with researchers from ASML, TNO ESI and TU Dortmund, we organized the Rigorous Examination of Reactive Systems (RERS) Challenge 2019, in which participating academic teams could test the limits of their verification tools using benchmark programs that were synthesized from models of ASML TWINSCAN components.

Our research received wide attention from peers. For instance, Vaandrager's survey on Model Learning appeared as a cover article in the Communications of the ACM in February 2017. It has been downloaded more than 16.5K times as of today, and has been translated in Chinese and Spanish. Vaandrager also gave invited lectures about model learning at international conferences e.g. ICALP'19, Highlights'17, RV'18 and ICGI'18.

In 2019, we set up a website https://automata.cs.ru.nl/ with a publicly available set of benchmarks of state machines that model real protocols and embedded systems to allow researchers to compare

the performance of learning and testing algorithms. Our benchmarks have already been used, by researchers from l'Université Grenoble Alpes, the University of Sao Paulo, the University of Sheffield, the University of Leicester, Universidad Complutense de Madrid, Sabanci University, Graz University of Technology, IST Austria, the Indian Institute of Science Bangalore, and Kansas State University.

The successful applications of model learning also triggered the interest of theoreticians, leading for instance to a series of papers by SWS researchers in collaboration with researchers from UCL, Strathclyde University, and the University of Warsaw in which coalgebraic, categorical and nominal perspectives on automata learning are explored. An example of this line of work is the POPL'17 paper co-authored by Joshua Moerman, which presents an algorithm to learn nominal automata. This paper influenced subsequent work by leading theory researchers such as D'Antoni, Tzevelekos, Schröder, and Bojańczyk. An example showing that theoretical work also leads to practical applications is L#, a new and simple approach to active automata learning that we recently developed. Instead of focusing on equivalence of observations, like the well-known L* algorithm and its descendants, L# tries to establish apartness, a constructive form of inequality. The notion of apartness is standard in constructive real analysis and goes back to Brouwer. Work on L# was inspired by a study of apartness by iCIS researchers Herman Geuvers and Bart Jacobs in the context of concurrency theory. Experiments with a prototype implementation of L#, written in Rust, suggest that it outperforms existing approaches.

Our work on model learning shows that setting up collaboration chains all the way from theory to practical applications can be quite effective. It helps to obtain a better understanding of when and how software science may help to solve real-world problems, and researchers from different areas benefit from each other's expertise. Applied researchers (from academia and industry) are challenged to try out new approaches to solve practical problems, and theoreticians are challenged to develop theory that is actually useful.

B.2 Real-World Crypto

Real-World Crypto research at iCIS focuses on the design and implementation of cryptographic techniques to cover a wide range of applications:

- Symmetric cryptography to protect bulk data in transit and storage; and
- Asymmetric cryptography for key agreement and cryptographic signatures.

Apart from publishing our results at academic venues, we also submit our designs to international standardization efforts, build prototypes, and write code that we make available open-source.

Symmetric cryptography

In symmetric cryptography we target lightweight (authenticated) encryption where low energy consumption in dedicated hardware is the primary goal. Energy consumption is crucial for battery life in low-end devices and often the bottleneck in contactless devices. In high-throughput encryption it determines the heat production and as such the achievable bandwidth. The challenge is to get high security assurance at low energy costs. We achieve this by cryptanalysis and a good understanding of attack complexities.

Traditionally, block ciphers are the central primitive of symmetric crypto and their design goal is to behave like a random permutation when loaded with an unknown key: PRP security. We introduced a new primitive to replace the block cipher: the deck function. It has arbitrarily extendable input and output and instead of a random permutation its ideal counterpart is a random oracle. This refactoring of symmetric cryptography leads to much simpler proofs for (authenticated) encryption modes and an over-all gain in energy-efficiency. We build deck functions in turn from cryptographic permutations using constructions such as duplex and farfalle. For these permutations we adopt lightweight bit-oriented components giving rise to low latency circuits and fast software.

Many applications require protection against adversaries that have physical access to the crypto-hosting device or can measure computation times and hence get side-channel information. We have developed modes on top of our duplex construction that offer resistance against power/electromagnetic side-channel attacks, avoiding the need for expensive algorithmic countermeasures such as masking. Our permutations on the other hand lend themselves for constant-time code eliminating the timing side channel.

While still in its infancy, our approach has led to a large following with many competitors in the NIST competitions for authentication encryption (CAESAR) and the NIST lightweight competition adopting our ideas.

Public-key cryptography

Until recently key agreement and cryptographic signatures were quite established with algorithms based on the difficulty of factoring and discrete logarithms over elliptic curves providing high security assurance for a modest cost.

The main challenge for these algorithms is to have bug-free implementations offering resistance against side-channel attacks, as discussed at the end of this case study. However, the security of all these algorithms is threatened by the possibility of quantum computers that would be capable of practically computing the private keys from their public counterparts by efficiently factoring large integers and solving discrete logarithms. While scuh quantum computers are still hypothetical, standardization bodies recommend to flee forward and migrate to new public-key cryptography that will resist them: so-called post-quantum cryptographic algorithms. The acceptability of these

algorithms depends on their trade-off between computational efficiency and communication overhead on the one hand and their security assurance on the other.

Our work focuses exactly on this trade-off for all 5 realms of post-quantum crypto: lattices, codes, hashing, isogenies and multivariate systems. We concentrate on efficient constant-time code and hardware architectures including hardware-software co-design. As in symmetric crypto, in post-quantum cryptography we are bringing our specific approaches to the standards by participating in the NIST post-quantum cryptography competition: with great success, as 5 of the 7 finalists have co-authors from the Digital Security group.

Public-key crypto code is challenging to implement correctly with generally more subtle bugs than symmetric crypto. We address this problem with formal verification from low-level code all the way up to the mathematical specification, in collaboration with formal methods researchers in the Software Science group. For pre-quantum algorithms we succeeded in such a verification effort for an implementation of the widely used X25519 key-exchange protocol. The formal verification of post-quantum cryptography is an ongoing effort and one of our focus areas in the future.

B.3 Causality for Psychology

Uncovering the Central Role of Inattention in Psychological and Behavioural Disorders

This case study covers how research into causality in the Data Science section has helped colleagues in psychology to uncover the central role of inattention in various psychological and behavioural disorders, and how this joint research resulted in both important new developments in causal methodologies *and* promising new insights and hypotheses for the psychology domain.

In 2016 we published an article [1] showcasing the surprising, and at the time quite controversial, finding that so-called inattention turned out to play a much more central role in ADHD than previously thought. Until then most neuropsychologists and experts in ADHD – the well-known acronym for Attention Deficit Hyperactivity Disorder - considered the two key facets hyperactivity/impulsivity and inattention essentially as two complementary aspects of a single complex condition, where the first was thought likely to be the more prominent factor in relation to other comorbidities such as behavioural disorders.

The research, carried out by PhD candidate Sokolova, built upon earlier theoretical work in causal discovery in our group, and found strong evidence that inattention was in fact much more fundamental to the condition, with hyperactivity to a large extent appearing as a side-effect of the first. The findings could be replicated across different cohorts and different age groups. Although still unclear about the precise mechanism behind this link, if true this could have significant impact on potential new treatment options in clinical settings.

Equally interesting, and perhaps even more surprising, was the finding that inattention *also* appeared to play a central role in aggression in mild behavioural disorders such as Oppositional Defiant Disorder (ODD) and more serious forms such as Conduct Disorder (CD). Although the link was initially not as strong as for ADHD, the implications could be even more far-reaching as behavioural disorders are notoriously difficult to treat.

Understanding and confirming this link was one of the goals of the MATRICS project [2], consisting of a large European consortium of research institutes headed by the Radboud University under the leadership of PI Glennon. Data Science at iCIS participated in the project and was responsible for developing new machine learning methods to support the integral data analysis and building a single coherent causal model that explained the combined results of the various sub-projects involved.

Our group was involved in developing several methodological breakthroughs needed to handle the highly challenging and diverse range of data sets available in the project, ranging from different surveys and clinical assessments all the way to genetic information, brain metabolites and medication trials. For example, in collaboration with colleagues Mooij (UvA) and Magliacane (IBM/VU) we published the novel Joint Causal Inference framework [2] that allowed us to combine results from different experiments in a principled and unified way. Prior to that a new Bayesian approach developed by PhD candidate Cui [3] helped us analyse results from different questionnaires, and another collaboration on causal domain adaptation [4] was crucial in comparing results over multiple cohorts. All of these (and others) were published in top tier journals and conferences.

Ultimately, we managed to confirm the central role of inattention for aggression in several independent ways. For example, it was experimentally verified in mouse behavioural studies in simulated environments involving mouse strains genetically prone to aggression. It was found consistently in large public cohort studies such as the ALSPAC data set (>15k participants) and other, new data sets. It could also provisionally be confirmed in preliminary results from medication trials conducted within MATRICS (although definitive results have been delayed due to Covid).

More importantly, the resulting coherent causal model seemed to suggest that there are in fact two different kinds of inattention that each played a distinct role in the relation to aggression: inattention in the form of a 'predisposition to misreading (social) cues' is linked to so-called reactive aggression and ODD, whereas a more deliberate 'rule-breaking' form of inattention is involved in increased proactive aggression leading to more serious forms of conduct disorders. In addition, it became clear that other potential important contributors such as anxiety and substance abuse are indeed strongly linked to several conditions, but appear mostly in the periphery of the model, indicating that they are most likely a consequent rather than a key initiating driver of various psychological and behavioural disorders. These novel insights from our causal modelling approach are considered so promising that they are intended to become the subject of a new follow-up project (to be submitted with Glennon), designed to confirm or disconfirm the hypotheses from the MATRICS project completed last year.

In reflection: this 'case study' exemplifies our approach to realising one of the research goals of Data Science at iCIS: bridging the gap between state-of-the-art causal discovery in theory and actual applications in practice. We do this by working in close collaboration with researchers from different areas of science on challenging real-world problems. Our role is to adapt and extend existing machine learning techniques, and help researchers to apply them to their experiments. This, in turn, helps researchers to (hopefully) gain new insights in their data and develop new hypotheses for further studies. At the same time, we gain invaluable information on the needs of specific application domains, and where current methodologies fall short. This stimulates new theoretical developments that can subsequently be applied to other experiments. All this with the overarching goal of unlocking the potential of modern, principled causal inference to the wider scientific community.

References

[1] Sokolova, Elena, Perry Groot, Tom Claassen, Kimm J. van Hulzen, Jeffrey C. Glennon, Barbara Franke, Tom Heskes, and Jan Buitelaar. "Statistical evidence suggests that inattention drives hyperactivity/impulsivity in attention deficit-hyperactivity disorder." PLoS one 11, no. 10 (2016): e0165120.

[2] J. Glennon et al. "Multidisciplinary Approaches to Translational Research In Conduct Syndromes (MATRICS)", call FP7-HEALTH-2013-INNOVATION, subcategory HEALTH.2013.2.2.1-3: Paediatric conduct disorders characterised by aggressive traits and/or social impairment: from preclinical research to treatment

[3] Cui, R., Bucur, I. G., Groot, P., & Heskes, T. (2019). A novel Bayesian approach for latent variable modeling from mixed data with missing values. Statistics and Computing, 29(5), 977-993.

[4] Mooij, J.M., Magliacane, S., & Claassen, T. (2020) "Joint Causal Inference from Multiple Contexts". Journal of Machine Learning Research, 21, 1-108.

[5] Magliacane, S., van Ommen, T., Claassen, T., Bongers, S., Versteeg, P., & Mooij, J. M. (2018). Domain Adaptation by Using Causal Inference to Predict Invariant Conditional Distributions. In Advances in Neural Information Processing Systems (NeurIPS), 10846-10856

B.4 Machine Learning, Security, and Privacy

The rise of AI means that machine learning is ever-more important for security and privacy. Machine learning can be a powerful tool to compromise security and privacy but can also be used for countermeasures against attacks. This case study covers the recent contributions that iCIS has made in using machine learning to attack and to defend systems and discusses the strategy that we pursue to encourage these new topics to take root in the larger research community. As iCIS we are uniquely positioned to carry out research in the intersection of Machine Learning, Security and Privacy by combining the expertise of the Data Science (DaS) and Digital Security (DiS) groups.

Machine learning as an attacker

Security evaluation labs are facing new challenges as adversaries become more powerful, based on the growing availability of resources, and also more advanced in terms of the methods and techniques they use. Our work has demonstrated that a side-channel attacker is capable of reverse engineering proprietary information from an ARM Cortex-M3 microcontroller, which is a platform often used in edge devices using neural networks such as wearables, surveillance cameras (Batina et al. 2019) and also from GPUs that are used in automotive for, e.g., high definition maps. Further, in 2017 we established a collaboration between DaS and DiS, which has led to the introduction of *ScreenGleaning*, a new TEMPEST attack that uses an antenna and software-defined radio to capture an electromagnetic side channel, i.e., emanations leaking from a mobile phone (Liu et al., 2021).

Machine learning as defense

Within iCIS, we have developed algorithms that demonstrate the ability of automatic classifiers to extract scene information from social media images (Zhao and Larson 2018). Such algorithms pose a privacy threat to users sharing images on social media. To address this threat, we have developed techniques that use neural networks to modify images in order to inhibit automatic classification. In 2018, this work was recognized with an Open Mind award from NWO, which provided the basis for establishing a research line on using machine learning for privacy defense in social media at iCIS. The results of the project are presented at: https://pixelprivacy.github.io and a key publication is Zhao et al. (2020).

Encouraging new topics to take root

The health and success of security and privacy research is dependent on researchers' ability to anticipate new threats and to develop creative solutions. With our research at the intersection of machine learning, security and privacy, we aim to enlarge the field, rather than focusing on trendy topics that already receive sufficient research attention. To this end, we need to develop new topics and encourage them to take root in the research community.

We have two main strategies that we use to pursue this goal. First, we work to develop new threat models (i.e., specifications that include the objectives of an attack and the resources at the disposal of the attacker). The Screen Gleaning attack is a prime example: until now, this type of attack had not been carried out and the research community did not have a specification of the possible parameters. Our work not only demonstrated the attack, but also presented a framework in which to define threat models.

Second, we develop testbeds and benchmarks, which provide data sets and specifications that make possible the fair comparison of new approaches. Such resources are critical to the community in order to carry out research that demonstrates that a new approach (e.g., a countermeasure) conclusively outperforms existing approaches. An example is the testbed that we released in order to enable the systematic evaluation of Screen Gleaning attacks. Another example is the Pixel Privacy task that we organized at the MediaEval benchmark (Larson et al. 2018). During the three years the

task was offered, 11 different teams participated from all over the world including Singapore, Vietnam, and France. The MediaEval benchmark is an example of Open Science, because it makes data, approaches, and results openly available.

In sum, our work has focused on gaining insight into how machine learning can threaten, but also support, security and privacy. Our research efforts place a special focus on defining new threat models as well as offering the benchmarks and testbeds in order to allow the new topics that we investigate to take root and establish themselves in the research community.

References

L Batina, S Bhasin, D Jap, S Picek. 2019. CSI NN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel. USENIX Security Symposium 2019: 515-532.

M Larson, Z Liu, S Brugman, Z Zhao. 2018. Pixel Privacy: Increasing Image Appeal while Blocking Automatic Inference of Sensitive Scene Information. Working Notes Proceedings of the MediaEval 2018 Workshop. Sophia Antipolis, France, 29-31 October 2018. http://ceur-ws.org/Vol-2283/MediaEval_18_paper_7.pdf

Z Liu, N Samwel, L Weissbart, Z Zhao, D Lauret, L Batina, M Larson. 2021. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. The Network and Distributed System Security Symposium (NDSS).

Z Zhao and M Larson. 2018. From Volcano to Toyshop: Adaptive Discriminative Region Discovery for Scene Recognition. In *Proceedings of the 26th ACM international conference on Multimedia* (*MM '18*). Association for Computing Machinery, New York, NY, USA, 1760–1768.

Z Zhao, Z Liu, M Larson. 2020. Towards Large Yet Imperceptible Adversarial Image Perturbations With Perceptual Color Distance. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1039-1048.

B.5 Interdisciplinary Collaboration and Societal Impact with Radboud iHub

iHub is Radboud's interfaculty research hub on digitalization and society. It was launched in May 2019 and is located at a central location of the university campus. iCIS is a launching partner of iHub, esp. via the close involvement of Prof. Bart Jacobs as one of the iHub directors, together with Prof. Tamar Sharon (in philosophy of technology). The university board has provided iHub with 6M initial funding, for a five year period, to be followed by an evaluation.

iHub has research collaborations with all of the university's Faculties, for instance in the form of joint PhD positions or in the form of part-time secondments from Faculties to iHub. Six staff members from the Faculty of Science (especially iCIS) are affiliated with iHub. An important aspect in the functioning of iHub is the physical proximity and scientific interaction between its researchers from different disciplines, based on bottom-up enthusiasm, instead of top-down directives. (The Covid restrictions have been a hard hit especially in iHub's interdisciplinary community-forming activities.)

iHub has no teaching tasks and fully concentrates on interdisciplinary research and outreach. iHub harbours an "iLab" for experimentation and translation of research activities into technical design and development, with ongoing and past projects on, for instance: privacy-friendly identity management (IRMA), local digital voting, encryption of files and email, dark patterns in user interaction, fighting disinformation, privacy-friendly Covid presence registration. iHub's research profile is characterized by:

1) its broad interdisciplinarity, spanning the humanities, engineering and social sciences;
2) a value-driven research agenda that focuses on how to secure public values in digitization processes;
3) a critical and constructive approach to societal challenges raised by digitalization.

These characteristics distinguish iHub from similar initiatives at the national and international level.[19]

Within iHub research on digitalisation is put in a wider interdisciplinary context, with a focus on four fundamental values that are at stake in the ongoing digitalisation of society. These are privacy & security; solidarity & justice; autonomy & freedom; knowledge & expertise. These values are relevant in studies on, for instance: technical and legal aspects of privacy and dataprotection; the legal and ethical aspects of AI, including risks of discrimination; the ethical and societal challenges associated with the entrance of large consumer technology companies such as Alphabet (Google), Apple and Amazon into the domain of health and biomedical research.

Via these broad interdisciplinary research activities iHub acts as a force multiplier for iCIS. iHub's outreach is very strong with several of its members (also from iHub) actively participating in societal discussions, in the media, and in advice boards. Two example topics illustrate this impact, where iCIS researchers at iHub (Zuiderveen Borgesius and Jacobs) have been involved.

First, Zuiderveen Borgesius has authored several publications regarding discrimination-related risks of AI, including an influential report for the Council of Europe (47 member states) Discrimination, Artificial Intelligence and Algorithmic Decision-Making. In the report, he gives advice for the short term: how existing non-discrimination law can be enforced more effectively when AI has discriminatory effects. He also gives suggestions for the longer term: how the law can be improved to protect people against unfair discrimination by AI. The Parliamentary Assembly of the Council of Europe cites the report in a draft Recommendation on "Preventing discrimination caused by the use

[19] In October 2021, Jacobs was awarded the NWO Stevin Prize, the highest (laureates receive 2.5M€) award and most prestigious recognition of science with impact in The Netherlands.

of artificial intelligence". On AI and discrimination and related topics, Zuiderveen Borgesius has also presented at, for instance, a course for European judges, the European Consumer Organisation, the Dutch Parliament, the European Parliament, and the Council of Europe. He is regularly asked for comments by the media, such as (nationally) De Volkskrant, NRC, Nu.nl, and The public broadcaster's TV news, and (internationally) Bloomberg, The Guardian,The Markup, and the Wall Street Journal.

Second, in April 2020 Jacobs published the article Maximator: European signals intelligence cooperation, from a Dutch perspective in the journal of Intelligence and National Security. It describes the existence of a previously unknown, independent, influential European network of five countries called "Maximator", existing besides the well-known Anglo-Saxon Five Eyes signals intelligence network. The Maximator cooperation was so secret that its existence remained unknown for 50 years. The paper contains a revelation of global importance which has already changed the field: it gives a whole new perspective on international power blocks and dependencies (less US, more EU-centered) and will have a profound impact on future intelligence studies. The article's impact was immediate: it had over 60.000 downloads within three months (by far the most in the journal's entire history) and was covered in the international press: The Economist (A beery European spy club is revealed), Le Monde, Frankfurter Rundschau, Berlingske. Independently of this publication, Jacobs served in 2020 as (sole technical) member of an influential and sensitive government committee that evaluated the 2017 intelligence law in The Netherlands (which was rejected earlier in a national referendum). The committee's report was published in January 2021, fully accepted by the government and forming the basis for an ongoing revision of the law.

For more information, see: https://www.ru.nl/ihub/

B.6 Building ecosystems for AI research and applications

Artificial Intelligence (AI) is one of the important research areas for the institute. This is obvious for the Data Science department, with its strong focus on machine learning and information retrieval research (as discussed in B.3). But AI research also features in the Software Science and Digital Security, e.g., on the application of AI to side-channel analysis (as discussed in B.4). Traditionally, and comparable to other academic institutions these days, AI research at the Radboud University is spread across the campus. Other strongholds include the Faculty of Social Science, which has a tradition on cognitive approaches to artificial intelligence and coordinates our university's bachelor and master programmes in AI, the medical faculty within the RadboudUMC, which among others hosts a leading group on medical imaging, and the Faculty of Arts, with a strong tradition on AI for text and speech analysis.

To better coordinate, position, and profile our research activities on AI across campus, we started the interfaculty initiative **Radboud AI**. Radboud AI's main theme is "AI for Life", which nicely connects to the profile of the region (#lifeport) and supports the societal engagement and broad orientation of the Radboud University and RadboudUMC. Through this initiative we secured two tranches of funding from our university's central board, to support and strengthen interfaculty AI research. One of our instruments is a voucher program to stimulate novel collaborative AI research. This led to various new initiatives, many of which involve iCIS researchers, such as a joint workshop with NEDAP on sharing healthcare records written in Dutch, a collaboration with the department of Ecology and Deltares on the use of deep neural networks for the detection of manmade structures (specifically dams) in satellite images, and highly interdisciplinary research on the perception of AI-driven decision making by the general public.

Through Radboud AI, we applied for and got assigned a prestigious ELLIS unit, one of the thirty in Europe and three in the Netherlands. ELLIS units bring together the best AI researchers at their locations and fulfill a set of criteria to ensure excellence and to be maximally competitive at the international level. With three senior members, iCIS is the purveyor of the board of the Radboud ELLIS unit. With the ELLIS unit in Prague, we share two PhD candidates who work on the improvement of automated theorem proving with novel machine learning techniques. The ELLIS PhD and postdoc program offers excellent opportunities for our junior researchers to increase their network and learn from the best AI researchers across Europe.

To strengthen collaboration with industry and societal partners, we set up several so-called ICAI (Innovation Center for Artificial Intelligence) labs. iCIS researchers are strongly involved in three out of the five ICAI labs in Nijmegen. The societal AI for Health lab aims to bring AI solutions into the clinic, the AI for Precision Health, Nutrition and Behavior develops AI algorithms and models to improve personalized lifestyle feedback, and the AI for Risk Profiling and Decision Support (AI-RONDO) lab focuses on AI methods for the detection and monitoring of symptoms related to neuro-degenerative conditions. Two iCIS members act as co-directors of these labs, which further involve various iCIS PhD candidates and postdocs. Example projects include MIHRacle (Multi-modal Interactive Health Records) on (semi-)automatic methods to open up the information from electronic patient records to patients, and MOCIA (Maintaining Optimal Cognitive function In Ageing) on multisource machine learning to predict biomarkers for cognitive decline. We expect to open several additional ICAI in the upcoming years, also outside of the health domain.

Together with Twente University, Radboud AI took the initiative to set up an AI hub in the eastern part of the Netherlands, soon joined by Wageningen University, the regional universities of applied sciences, several regional economic boards, and the development agency Oost NL. Within a short time, the AI-hub Oost-Nederland became the AI ecosystem in the region and is now one of the seven

hubs that are part of the Netherlands AI coalition (NL AIC). Many iCIS researchers are involved, e.g., as academic representatives for one of the application domains. On a slightly smaller scale, we contributed to the creation of the AI for Life center of the Economic Board Arnhem-Nijmegen (with Wageningen). Through these ecosystems, we build closer connections between the various academic and non-academic partners, discuss joint interests, and prepare for potential funding opportunities, e.g., through the national AINED growth fund resources and Horizon Europe.

To summarize, through the Radboud AI initiative, iCIS is excellently connected and embedded in various AI ecosystems. ELLIS, and to a lesser extent CLAIRE, provide an international network for (mainly) core machine learning research. The NL AIC with the AI-hub Oost-Nederland, the ICAI labs, and the AI for Life center, connect us to industrial and societal partners on a national and regional scale for (predominantly) more applied AI research. Our efforts to build these networks have already paid off in the form of novel collaborations and exciting new research, most notably on machine learning and information retrieval in the biomedical domain, but also increasingly with other industrial and societal partners.