MASTER OF SCIENCE IN CYBER SECURITY

LEIDEN UNIVERSITY

February 2020

Contents

Summary 3

Report on the Master of Science in Cyber Security of Leiden University 5

Administrative data regarding the programme 5

Administrative data regarding the institution 5

Composition of the assessment panel 5

Working method of the assessment panel 6

Assessment per standard 7

Standard 1: Intended learning outcomes 7

Standard 2: Teaching-learning environment 8

Standard 3: Student assessment 12

Standard 4: Achieved learning outcomes 14

General conclusion 15

Recommendations 15

Overview of the Assessments 17

Annexes 18

Annex 1 Programme of the site visit 19

Annex 2 Documents reviewed 20

Annex 3 Abbreviations 21

Summary

Intended learning outcomes

The Master of Science in Cyber Security is a multidisciplinary programme at the post-Master level, covering relevant technical, governance, business and regulatory elements. It aims to educate cyber security professionals who are able to look beyond the limits of their own disciplinary background and see the bigger picture of the cyber security issues that confront their organisation. The Master is a unique and pioneering programme, updated continuously to reflect the developments in the academic and professional field. The panel advises the programme to state its position in relation to academic and professional standards and frameworks more explicitly, thus clarifying to academia, the professional field, potential students and their employers what it does and does not offer. Students choose for the technical or the governance track as their specialization. The technical track's learning objectives are useful and sufficiently challenging for students with a non-technical background, but could be more ambitious for those with a technical background.

The Master of Science in Cyber Security meets standard 1.

Teaching-learning environment

The Master Cyber Security is a two-year part-time programme and consists of four semesters of 15 EC each. The programme is developed for professionals in (cyber) security with a technical or a governance background. The first semester offers all students the same encompassing perspective on cyberspace and the security challenges. It provides an overview of cyber security issues and solutions as these are studied in a variety of disciplines. Next, students enter one of two specialisations: the governance or the technical track. The third semester largely consists of electives, giving students the opportunity for further specialisation. In the fourth semester, students demonstrate their acquired knowledge and skills by conducting independent, original research, which is written down in a thesis.

The panel assesses the Master Cyber Security as an excellent learning environment, with clear educational objectives, interactive teaching and diverse assignments. The programme stimulates further thinking and development. The link with professional practice is strong and students can apply their knowledge and skills immediately. The programme is well-run with strong feedback loops from students, Board of Examiners and alumni. Continuously adapting the programme to students' needs is a good thing, but it reduces the predictability of the programme. These changes are part of a new programme. For the future, the panel advises to carefully balance student feedback against other inputs. The number of elective courses in the technical track is limited. The panel recommends adding one or two, e.g. on Artificial Intelligence and blockchain. A study visit abroad would also be a useful addition to the programme.

The panel considers the use of English as the programme's working language fully justified. The programme has set up a careful intake selection. In previous student cohorts, the level of academic writing in English was a point of attention, but this seems to have been addressed by updating the intake procedure. The panel advises to encourage more international students to enroll.

Most teaching is carried out by core lecturers from Leiden University and Delft University of Technology. All of them are active academic researchers and didactically qualified. Students confirmed in the interview that the quality of the lecturers is high. Guest lecturers are appreciated because they add the perspective of the fast changing field of cyber security and bring a lot of value on specific topics. The panel agrees that the teachers' expertise is outstanding, but notices an outflow of lecturers with a technical background. This needs to be reinforced. The panel notes some concerns with guest lecturers, such as the coordination of their input and quality differences in their presentation skills. The programme has good feedback mechanisms, but ensuring the quality of guest lecturers is still a challenge. The panel recommends inviting more guest lecturers from the public sector.

The Master of Science in Cyber Security meets standard 2.

Student assessment

The system of student assessment is consistent and of high quality. Lecturers use a diversity of assessment methods. The quality of exams and assignments is stimulated by clear guidelines and the four-eyes principle, and is verified by the Board of Examiners. The Board of Examiners fulfills all duties required by law and takes its responsibilities seriously, as was illustrated by the minutes of its meetings and the interview with the panel. Overall, the assessments are of the appropriate level, but the panel feels that some exam questions are a bit too easy. The panel suggests to introduce in-class open-book exams, with less emphasis on reproduction and more on application of knowledge.

Feedback provided to students is satisfactory for assignments and generally for theses as well, although students note that timely feedback differs between supervisors. The detailed rubric for the thesis assessment is very good and helps to overcome cultural differences between disciplines. For further improvement, the panel advises that examiners motivate their grade by adding text on the assessment form. In view of the multidisciplinary nature of the theses, the panel thinks it would be useful to have an examiner other than the main supervisors, e.g. the track coordinator, to guarantee the multidisciplinarity and the consistency of grading within a track.

The Master of Science in Cyber Security meets standard 3.

Achieved learning outcomes

The panel studied a selection of fifteen theses and the accompanying assessment forms, to assess whether the intended learning outcomes are achieved. The theses are generally proof of well-executed research with good research questions and sound methodology. In some theses, the use of English is a problem. These language issues are expected to decrease, because the intake procedure now pays more attention to the level of English and academic writing of candidates. The panel generally agrees with the given grades, with the exception of one thesis that is deemed sub-standard. One thesis is satisfactory, but very short (22 pages excluding appendices). The panel thinks it is advisable to not only define a maximum length in the thesis guidelines, but also a minimum. This will do justice to the amount of work required. Other theses are very good or even outstanding. They provide detailed and well written texts with extensive references and critical analysis. One thesis was an excellent monodisciplinary piece of work. The panel feels that all students ought to include at least a short section to illustrate the multidisciplinary nature of the learning outcomes, e.g. a reflection on ethical aspects in a technical thesis. The alumni are very enthusiastic about the programme and its practical use in their profession.

The Master of Science in Cyber Security meets standard 4.

Conclusion

The programme meets all standards. The panel assesses the Master of Science in Cyber Security as ‘positive’.

The chair and the secretary of the panel hereby declare that all panel members have studied this report and that they agree with the judgements laid down in the report. They confirm that the assessment has been conducted in accordance with the demands relating to independence.

Date: 13 February 2020

Prof. dr. Ir. Bart Preneel
(Chair)

Dr. Marianne van der Weiden
(Secretary)

Report on the Master of Science in Cyber Security of Leiden University

The panel has based its assessment on the standards and criteria described in the NVAO Assessment framework for the higher education accreditation system of the Netherlands (Stcrt. 2019, nr 3198).

Administrative data regarding the programme

Name of the programme:	Cyber Security
CROHO number:	75120
Level of the programme:	master of science
Orientation of the programme:	academic
Number of credits:	60 EC
Specialisations or tracks:	Technical track; Governance track
Location:	The Hague
Mode of study:	part-time
Language of instruction:	English
Expiration of accreditation:	29 January 2021

The visit of the assessment panel took place on 16 January 2020.

Administrative data regarding the institution

Name of the institution:	Leiden University
Status of the institution:	Publicly funded institution
Result institutional quality assurance assessment:	positive (2019)

Composition of the assessment panel

The panel that assessed the master of science programme in Cyber Security consisted of four members:

- Prof. dr. ir. Bart Preneel, full professor Computer Security and Industrial Cryptography, KU Leuven, Belgium (chair);
- Prof. dr. Jeanne Pia Mifsud Bonnici, full professor in European Technology Law and Human Rights, Faculty of Law, Rijksuniversiteit Groningen;
- Liesbeth Holterman MA, independent cyber security consultant;
- Hamidreza Mojab MSc, doctorate student at Delft University of Technology (student member).

The panel was supported by dr. Marianne van der Weiden, who acted as secretary.

The NVAO approved the composition of the panel in November 2019.

Working method of the assessment panel

Preparation

The panel members prepared the assessment by analysing the self-evaluation report and the appendices provided by the institution. The panel members formulated their preliminary findings and questions. The secretary made an overview of these preliminary findings and sent it to the panel members as a preparatory document. The panel members also requested additional information, that was delivered in electronic form several days before the site visit.

The panel also studied a selection of fifteen master theses and the accompanying assessment forms for the programme, based on a provided list with theses of the last two years. This selection was made by the panel's chair and secretary, who took care that a variety of topics was covered and made sure that the distribution of grades in the theses selection included equal numbers of high, intermediate and low grades.

The panel held a preparatory meeting on 15 January 2020, i.e. the day before the site visit. During this meeting, the panel was instructed regarding the assessment framework and procedure. After this, the panel discussed its working method, its preliminary findings and formulated the questions and issues it wanted to discuss with the programme's representatives during the site visit. The panel also reviewed the assignments and exams provided.The panel chair, secretary and programme jointly composed a schedule for the site visit. Prior to the site visit, the programme selected representative partners for the various interviews. See Annex 1 for the definitive schedule.

Site visit

The site visit took place on 16 January 2020 at Campus The Hague of Leiden University. During this visit, the panel was able to discuss the formulated questions and to gather additional information during several sessions (Annex 1: Schedule of the site visit). The panel also examined the additional materials provided by the programme. An overview of these materials is given in Annex 2.

Afterwards, the panel discussed the findings and considerations and pronounced its preliminary assessments per standard. At the end of the site visit, the initial findings were presented to the institution.

Report

Based on the findings, considerations and conclusions the secretary wrote a draft advisory report that was first presented to the panel members. After the panel members had commented on the draft report, the chair endorsed the report. On 27 January 2020 the advisory report was sent to the institution, which was given the opportunity to respond to any factual inaccuracies in the report. The institution replied on 10 February 2020 and asked for two corrections. The secretary discussed these with the panel's chair and adapted the report accordingly before its finalisation. The panel composed its advice in full independence.

Definition of judgements standards

The assessment is based on the standards and criteria described in the NVAO Assessment framework for the higher education accreditation system of the Netherlands (Stcrt. 2019, nr 3198). Fundamental to the assessment is a discussion with peers regarding the content and quality of the programme. Regarding each of the standards, the assessment panel gives a substantiated judgement on a three-point scale: meets, does not meet or partially meets the standard. The panel subsequently gives a substantiated final conclusion regarding the quality of the programme, also on a three-point scale: positive, conditionally positive or negative.

Assessment per standard

Standard 1: Intended learning outcomes

The intended learning outcomes tie in with the level and orientation of the programme; they are geared to the expectations of the professional field, the discipline, and international requirements.

Findings

The Master of Science in Cyber Security aims to educate cyber security professionals who are able to look beyond the limits of their own disciplinary background and see the bigger picture of the cyber security issues that confront their organisation. In the self-evaluation report, the Master Cyber Security is described as a multidisciplinary programme at the post-Master level, covering relevant technical, governance, business and regulatory elements. To do justice to the complexity of modern-day cyber security challenges, both in the public and private sector, the programme offers an integrated perspective on the topic. Students have prior experience and substantial knowledge in a sub-field or aspect of (cyber) security and, in the programme, gain high-level knowledge from a variety of disciplines and a solid understanding of the many facets that make up cyber security challenges. Thus, an organisation's technology experts, legal experts and management can communicate effectively with each other and work together to make informed decisions on cyber security problems, potential solutions and strategies.

Two scientific models underpin the programme's philosophy: (1) the three layer-model of cyberspace (technical, socio-technical and governance), and (2) the cyber harm model (in cyber space and/or the physical world, intentional/wilful and unintentional/accidental). Both models substantiate the multidisciplinary way of teaching cyber security. The programme is research-led and practice-oriented. The academic teaching staff consists of (inter)nationally renowned researchers. Students are taught the latest scientific insights and train critical thinking and academic writing skills. The programme seeks to make academic knowledge productive for the students' professional contexts. Students' real-world knowledge is used in courses to make these courses practically relevant and to facilitate the translation of academic theories and approaches to the professional realities of public and private organisations. Relevant case studies, policy papers, standards and binding legal instruments are analysed and discussed. Guest lecturers contribute their state-of-art knowledge and experience.

Students come from different disciplinary fields and professional backgrounds. In the first semester of the programme, all students are taught a unified shared outlook on cyberspace and cyber security. All key concepts are defined in the same way. The students' knowledge is synchronised to the same advanced level. After the first semester, students choose either the technical or the governance track.

The programme started in February 2015. It is taught collectively by teachers from Leiden University (LEI), Delft University of Technology (TUD) and The Hague University of Applied Sciences (THUAS). The collaborative teaching by staff members from several academic institutions contributes to the integrated perspective on cyber security. In the beginning, the collaboration was fuelled mostly by the enthusiasm of individual researchers from the three knowledge institutes. After the first years, the organisational pull of these institutes and the scarcity of resources and expertise led to the institutes withdrawing teaching staff. The programme management was able to staff the programme each year, but in order to ensure the continued joint teaching, Leiden University has engaged in negotiations for multiple-year staffing contracts with TUD and THUAS.

Cyber security is a rapidly developing field. In order to reflect the latest insights, the programme is continuously adjusted. In order to keep a connection with the full breadth of cyber security challenges, Expert Meetings are organised on a regular basis. These meetings are attended by professionals from the field, academics, core staff and (former) students. They are used (1) to get feedback from the field on the curriculum and teaching philosophy, (2) to have teaching staff engage with academic insights from other academic fields, and (3) to

obtain state-of-the-art knowledge from experts in the field on the latest developments and to evaluate whether or not these developments should be integrated into the programme.

The intended learning outcomes are described in appendices of the self-evaluation report. They are described in terms of the Dublin descriptors at master level. Schematic overviews show in which course or courses the learning goals are achieved. The learning goals reflect the substantive vision of the programme and specify which disciplinary knowledge is taught in this multidisciplinary programme.

Considerations

Based on the written documentation and the interviews during the site visit, the panel has gained a good insight in the vision and aims of the Master of Science in Cyber Security. The panel recognizes that the Master is a unique and pioneering programme, updated continuously to reflect the developments in the academic and professional field. The Expert Meetings are useful to remain up to date and they add to the networking opportunities for all involved (staff, professional field, alumni, students). The multidisciplinary character of the programme is clearly visible and is supported by the contributions from three knowledge institutes. The panel appreciates that more formal agreements are currently negotiated to guarantee the continuation of this joint teaching.

The panel observes that the level of programme is high. The learning objectives are a good indication of both the programme's multidisciplinary nature and the master's level. The panel feels that the intended learning outcomes for the governance track are more in line with the programme's ambitions than those for the technical track. Offering a technical track raises expectations. The technical track's learning objectives are useful and sufficiently challenging for students with a non-technical background, but could be more ambitious for those with a technical background. For students of both tracks, the panel advises to provide a broader technical background and an update on topics such as blockchain and artificial intelligence.

The panel agrees that the Master Cyber Security is a unique programme. The panel advises the programme to state its position in relation to academic and professional standards and frameworks more explicitly, thus clarifying to academia, the professional field, potential students and their employers what it does and does not offer. Relevant academic options are the framework of IEEE/ACM/IFIP (https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf), the leading international framework for academic programmes in cyber security, and the UK Cybersecurity Body of Knowledge (https://www.cybok.org/).

Conclusion

The Master of Science in Cyber Security meets standard 1.

Standard 2: Teaching-learning environment

The curriculum, the teaching-learning environment and the quality of the teaching staff enable the incoming students to achieve the intended learning outcomes.

Findings

Curriculum structure

The Master Cyber Security is a two-year part-time programme and consists of four semesters of 15 EC each. The programme starts in February, as opposed to other academic programmes that usually start in September, because the fiscal year fits the students' employers' budget cycle better than the academic year.

The programme is developed for professionals in (cyber) security with a technical or a governance background. The first semester offers all students the same encompassing perspective on cyberspace and the security challenges. It provides an overview of cyber security issues and solutions as these are studied in a variety of disciplines. Next, students enter one of two specialisations: the governance or the technical track. Each track consists of three courses, from broad and general to narrow and specific. The third semester largely consists of electives, giving students the opportunity for further specialisation. In the fourth semester, students demonstrate their acquired knowledge and skills by conducting independent, original research, which is written down in a thesis.

Contents

The programme covers the academic domains of public administration, organisational sciences, business administration, economics, philosophy, political science, computer science, law, criminology, psychology, sociology and (crisis) management and safety science. The first semester is designed to offer a broad view on cyber security, ensuring that all student acquire the same multidisciplinary knowledge, regardless of their own background or the track they will choose. In 2019, these courses were Introduction to Cyber Space, Cyber Risk Management and Cyber Risks & the Social Sciences.

The second semester starts with two short general courses (Legal Perspectives on Cyber Security and Cyber Security Economics), after which students enter the technical or the governance track. Both specialisations offer in-depth study of either the technical or governance aspects of cyber security. Basic technical (mathematical) knowledge is a prerequisite to be allowed to the technical track. Often, students with a background in technology choose the governance track in order to broaden their knowledge. The division between both tracks is roughly 1/3 (technical) versus 2/3 (governance). It appears from the interview with students that students with a hardcore technical background feel that the technical track is not technical enough.

The third semester consists of a mandatory course in each track (Case Studies in Cyber Security for the technical track, Cyber Security Governance for the governance track), followed by the choice of two elective courses from a list of four or five. The offer of electives was adjusted over the years based on the needs of the students and the availability of staff. Students' evaluations and requests may turn an elective course into a mandatory course for the next cohort, or lead to the development of a new course. It sometimes proves difficult to find a lecturer for a specific course, such as Data Mining for Cyber Security. Students told the panel that they consider the choice of technical electives to be too limited.

In the fourth semester, students write an academic thesis by developing a relevant research question and giving it in-depth scholarly treatment using a multidisciplinary approach. Supervision is provided by a thesis supervisor and a second reader. Thesis preparation days provide additional methodological training.

Language

The Master Cyber Security is internationally oriented, since cyber security is an international, borderless problem: both challenges and solutions are often international in nature. The programme falls within the responsibility of Leiden University's Faculty of Governance and Global Affairs. Most of this faculty's programmes have an international profile and are taught in English.

The programme draws from an international field of applicants. The percentage of international students fluctuates per cohort and is often modest. In its meeting with alumni, the panel heard that international students are seen as an enrichment of the learning environment.

A good command of the English language is one of the admission criteria for the Master Cyber Security. This is tested on the basis of an applicant's cv and motivation letter and in an individual interview with the Programme Director and Programme Coordinator. Lecturers must also have sufficient English competency. At the start of the programme, an English language skills training was provided to staff. New lecturers are asked to

provide a mini-lecture in English to make sure their level of English is sufficient. The English level is monitored in course evaluations and lecturers are replaced if there are reasons for concern in this respect.

All assessments are conducted in English. Despite the intake requirements, academic writing in English has proven challenging for some students, especially when writing the final thesis. The panel recognised this (see standard 4) and heard during the site visit that, in order to prevent such problems, the English language and academic writing requirements are checked more rigorously in recent years.

Intake

Admission is open to academic professionals who have completed a relevant master's programme (in the natural sciences, social sciences or the humanities) and have several years of work experience in the area of (cyber) security. Applicants must have sufficient competence in mathematics, methodology, English and academic writing. Potential students are interviewed by the Programme Director and the Programme Coordinator. In this interview, the commitment of the employer (if applicable), the expectations of the student and the registration process are discussed. Students are informed of the necessary time investment, the academic level and the vision behind the programme.

Professionals with a bachelor's degree can be admitted under the additional condition of an intake assignment, to test the applicant's level of English and academic writing. The assignment is assessed by the Programme Director (with a governance background) and one of the core lecturers (with a technical background). If necessary, applicants may be referred to (online) courses to improve their English and/or academic writing before the start of the programme. When the Master Cyber Security is expected to be too academic or difficult the student may be advised to enrol in another programme. Students are positive about the intake procedure.

Learning environment

Each cohort has a maximum of 24 students, in order to ensure the interactive nature of classes. In their meeting with the panel, the students emphasised the value of the programme for their professional life. They feel they can apply almost every course in their work immediately, e.g. by using their own context in assignments.

Students use the networking capacity of the programme by keeping in touch outside the classroom, and exchanging ideas and best practices when they encounter cyber security related challenges in their professional environment. Informal connections take place via social outings and Whatsapp groups, while more formal relationships are stimulated through the alumni network and the Expert Meetings (see standard 1). The alumni suggested in their meeting with the panel that an international study trip would be a useful addition to the programme, both in terms of bonding and to get acquainted with a range of organisations.

The programme is located in the building of the Hague Security Delta (HSD), a network organisation consisting of business, governments and knowledge institutions in the wider field of security. The expectation was that this environment would lead to constant (informal) meet-ups, but the cooperation is less intensive than hoped from the beginning. This is mainly because the programme's classes are organised on Fridays, when the building is almost empty. This is an item on the agenda of the programme's meetings with the HSD Board. Recently, the master's programme in Cyber Security Engineering of THUAS has started in the HSD building on the same day. This offers more opportunities for interaction.

The programme must abide with the regulations and procedures of LEI. This has sometimes led to frustration among students, as described in the self-evaluation report. Registration and payments are not in line with other programmes that start in September, which leads to administrative hiccups. Students would wish more flexibility, e.g. in deadlines, required presence in class and the mandatory nature of a course. Such issues have been addressed by a stronger dialogue between the programme management and the students (via the Programme Committee).

In general, the students told the panel that they find the management responsive to their needs. Students are invited to evaluate each course, teacher and assessment at the end of a course. They experience that their comments are taken seriously and lead to changes in programme and staff, if necessary.

Feasibility

The programme demands a time investment of approximately 20 hours per week. A minimum of six contact hours per week (on Fridays) is supplemented with supervision meetings and individual study. Students commit themselves to two years of this study load on top of their jobs and private life. The students who were invited to meet with the panel, agreed that the workload is significant and has an effect on their social life. This did not come as a surprise, since the required time investment was emphasised in the admission procedure. The students expressed that the effort is worthwhile for them, since the programme provides so much added value. Some of the students commented that it was their deliberate choice to invest a lot of time, because they aim for a high grade.

The programme is designed to be completed in two years. On average, 72% of students graduate within this time period. Drop-outs are exceptional, and most delayed students graduate at a later moment. The Programme Coordinator monitors the progress of every individual student and discusses how to prevent or reduce delays. Most delays occur in the period of thesis writing, when the structure of weekly class meetings is no longer there, or because student started their preparations too late. Therefore, thesis preparation days were introduced in 2018 during the third semester, offering workshops and guidance on writing, finding and citing sources and doing interviews. Students feel these days are helpful.

Staff

Most teaching is carried out by core lecturers from LEI and TUD. All of them are active academic researchers and have obtained their University Teaching Qualification (UTQ) or are in the process of doing so. Only a few of them are full professors (hoogleraar). Guest lecturers from THUAS and the professional field are engaged to teach particular subfields. The THUAS lecturers have obtained the Basic Teaching Qualification (BTQ) for lecturers from universities of applied sciences. Guest lecturers from the professional field are invited for their relevant experience in the industry and have a post-secondary level of knowledge and reasoning.

Most governance related courses are taught by LEI staff, while lecturers from TUD and THUAS teach the technical courses. The involvement of TUD and THUAS has decreased since 2018, due to retirement and increasing obligations of staff within their own institution. In order to complement the expertise of the core staff, guest lecturers come in from private companies and are involved in courses in technical aspects. As mentioned above (standard 1), the programme management has started negotiations with TUD and THUAS to ensure their future commitment. Additionally, the Leiden Institute for Advanced Computer Science (LIACS) has become involved and contributes an additional lecturer with a technical background. The programme management tries to hire new colleagues from private sector partners.

Lecturers from different disciplines often teach collaboratively, to ensure the multidisciplinary approach and programme coherence. In some courses, the number of guest lecturers is large. The choice for a range of different guest lecturers in the first semester is deliberate, because these courses aim to lay the groundwork broadly, before later courses go more in-depth. To ensure the coherence within a course with many guest lecturers, core staff is present in the lectures to introduce and summarise the guest lecturer's contribution and to maintain the narrative of the course. In order to avoid overlap, guest lecturers are briefed on the course, but this is not always sufficient, as is shown by the students' evaluations.

Students evaluate their teachers after every course. The outcomes are included in the self-evaluation report and are very positive. Students confirmed in the interview that the substantive and didactic quality of the lecturers is high. Lecturers are clear about the assessment criteria and their English level is good. Guest lecturers are appreciated because they add different perspectives and bring a lot of value on specific topics.

Their presentation skills differ. If necessary, this is discussed in the Programme Committee and a different guest lecturer may be invited next time.

Considerations

The panel has heard and seen that the Master Cyber Security provides an excellent learning environment, with clear educational objectives, interactive teaching and diverse assignments. The programme stimulates further thinking and development. The link with professional practice is strong and students can apply their knowledge and skills immediately. The Expert Meetings contribute to the strong networking environment.

The programme is well-run with strong feedback loops from students, Board of Examiners and alumni. Continuously adapting the programme to students' needs is a good thing, but it reduces the predictability of the programme. These changes are part of a new programme. For the future, the panel advises to carefully balance student feedback against other inputs.

The number of elective courses in the technical track is limited. The panel recommends adding one or two, e.g. on Artificial Intelligence and blockchain. A study visit abroad would also be a useful addition to the programme.

The panel considers the use of English as the programme's working language fully justified. The programme has set up a careful intake selection. In previous student cohorts, the level of academic writing in English was a point of attention, but this seems to have been addressed by updating the intake procedure. The panel advises to provide a scientific writing workshop prior to the thesis period for students who struggle with academic writing in English. The panel advises to encourage more international students to enroll. The many relevant international organizations in The Hague may offer useful recruitment opportunities.

The teachers' expertise is outstanding, but the panel notices an outflow of lecturers with a technical background. This needs to be reinforced. The panel notes some concerns with guest lecturers, such as the coordination of their input and quality differences in their presentation skills. The programme has good feedback mechanisms, but ensuring the quality of guest lecturers is still a challenge. The panel recommends inviting more guest lecturers from the public sector.

Conclusion

The Master of Science in Cyber Security meets standard 2.

Standard 3: Student assessment

The programme has an adequate system of student assessment in place

Findings

Student assessment in the Master Cyber Security is based on the Faculty Assessment Plan, the Course and Examination Regulations and the Rules and Regulations of the Board of Examiners. Assessments should be aligned with the learning objectives and a diversity of assessment methods is required. The self-evaluation report states that assessments in the Master Cyber Security are designed to assess students' ability to autonomously integrate knowledge, handle complexity and develop critical and objective conclusions on governance and technical issues of cyber security by using analytical techniques. Students must also demonstrate their ability to adequately communicate the results of their analysis.

Each year, lecturers submit a proposal for the assessment methods in their course. In every course with minimum of 5EC, at least two assessment methods are used, to ensure that different skills are assessed. Methods range from take-home exams or in-class written tests to assignments (individual or group),

presentations and the final thesis. Based on the lecturers' proposals, the programme management draws up an assessment plan with sufficient diversity in assessment methods. The Board of Examiners has an advisory role in the determination of the assessment plan. During the site visit, the panel studied exam papers written by students for a number of courses.

The validity of assessment is secured in two ways. Firstly, lecturers use a matrix to ensure that all learning objectives are assessed at the appropriate level, and, secondly, lecturers are encouraged to organise an a priori four-eye-review of their written exams. Model answers and answer keys enhance the reliability of grading of exams, while grading rubrics achieve this for assignments, papers and the final thesis. The Board of Examiners checks the exams and assignments including the model answers and grading rubrics.

Theses are supervised by joint teams of supervisors, often from different disciplines. Criteria about what a 'good' thesis is, differ between the natural sciences, social sciences and humanities. To make sure that such cultural differences do not affect a student's grade, an elaborate grading rubric and assessment form for theses has been developed. The assessment form also shows the weight of the different components that determine the final grade: quality of work (40%), process (30%), report (20%), presentation & defence (10%). The panel notes that there is (limited) space on the assessment form to provide feedback and substantiate the grade, but this possibility is hardly used. The Board of Examiners checks a sample of theses each year and has not identified any problems so far. It should be noted that the Board of Examiners is not able to verify the scores for process and presentation & defence. Students are informed about the methods of assessment in the e-prospectus at the beginning of the year and in the syllabi published on Blackboard for each course. After each exam, students can compare their work to the model answers or the grading rubric in an individual exam review session. Lecturers are present to explain and motivate the grades. The grading of the thesis is explained to the student after the defence and the announcement of the grade. Students generally appreciate the amount of feedback on assignments, although some would welcome more feedback, e.g. on academic writing, especially if their prior education was quite a few years ago. Alumni told the panel that getting feedback on time from thesis supervisors differs per student and partly depends on how active they are in asking for it.

Examiners are appointed by the Board of Examiners. All must have a doctorate degree or equivalent and must either have a UTQ or be in the process of obtaining this qualification soon. For THUAS this is the BTQ. Academic staff members without a doctoral degree are only appointed as examiners if there is a clear motivation, e.g. outstanding previous teaching evaluations or a demonstrable research expertise relating to the course content. Lectures without a UTQ may not perform the role of examiner independently. A thesis is examined by the supervisors. The second supervisor, who has been less involved in the process than the first supervisor, takes the lead in the examination procedure. If an additional supervisor from the professional field has been involved, this supervisor's role in examination is advisory. Examiners share their grades before the presentation and defence. The final grade is set after the defence and may shift marginally (plus or minus 0.5) on the basis of the quality of the defence. The rule is that, in case of disagreement between the examiners, a third examiner is appointed and determines the grade, on the basis of an independent reading. This situation has not yet occurred.

The Board of Examiners of the Master Cyber Security has three members, including an external member, and is supported by a professional secretary. Members are appointed by the Faculty Board for a period of two years with possible extension. The Board of Examiners covers expertise in all relevant areas (regulations, contents, assessments). The Board's role is to safeguard the quality, transparency and integrity of the examination process. It writes the Rules and Regulations, advises on the assessment plan and the Course and Examination Regulations, appoints examiners and determines whether a student has met the learning objectives at the end of the programme. If a student has passed all exams and procedural requirements have been met, the Board issues the diploma. The Board handles cases of fraud and plagiarism. Students have lectures and workshops on correct referencing and all written assignments are handed in through Turnitin, a plagiarism checking tool. When a case of suspected plagiarism is brought to the Board (this has happened a few times), a hearing with the student(s) involved is organised before a decision is taken. Each year, the Board of Examiners checks the level of theses by reading a sample with different grades and looking marginally at the assessment, without

knowing the grade. So far, no problems have been identified. When asked by the panel if the Board's expertise is broad enough to cover the range of topics in such a multidisciplinary programme, they responded that this is generally sufficient, but that, if necessary, they call on colleagues with more specific knowledge.

Considerations

The panel is satisfied that the system of student assessment is consistent and of high quality. Lecturers use very diverse assessment methods. The quality of exams and assignments is stimulated by clear guidelines and the four-eyes principle, and is verified by the Board of Examiners. Overall, the assessments are of the appropriate level but, based on the exam papers, the panel feels that some exam questions are a bit too easy. The panel suggests to introduce in-class open-book exams, with less emphasis on reproduction and more on application of knowledge.

Feedback provided to students is satisfactory for assignments and generally for theses as well, although students note that timely feedback differs between thesis supervisors. The detailed rubric for the thesis assessment is very good and helps to overcome cultural differences between disciplines. For further improvement, the panel advises that examiners motivate their grade by adding text on the assessment form. Without such text, it is not possible for the Board of Examiners to check two of the four criteria (process and presentation & defence) when they evaluate the annual sample of theses. In view of the multidisciplinary nature of the theses, the panel thinks it would be useful to have an examiner other than the main supervisors, e.g. the track coordinator, to guarantee the multidisciplinarity and the consistency of grading within a track.

The Board of Examiners takes its responsibilities seriously, as was illustrated by the minutes of its meetings and the interview with the panel.

Conclusion

The Master of Science in Cyber Security meets standard 3.

Standard 4: Achieved learning outcomes

The programme demonstrates that the intended learning outcomes are achieved.

Findings

The master thesis is the concluding aptitude test. All stages of an academic research project must be followed and are part of the assessment: formulating a relevant research question, literature review, methodology, analysis and conclusion. The thesis must include independent research. A strong focus, coherence, consistency and an accurate research goal are emphasised during the programme as the essential components of a good master's thesis.

In preparation for the site visit, the panel studied a selection of fifteen theses and the accompanying assessment forms. The distribution of grades in the thesis selection included equal numbers of high, intermediate and low grades and the selection covered a variety of topics. The panel appreciates that almost all theses show a good relation to their research question and that the use of methodology is thorough and sound. Differences between disciplines are visible in e.g. the literature reviews. In some theses, the use of English is a problem. The panel generally agrees with the given grades, with the exception of one thesis that is deemed sub-standard. One thesis is satisfactory, but very short (22 pages excluding appendices). Other theses are very good or even outstanding. They provide detailed and well written texts with extensive references and critical analysis. One thesis was an excellent monodisciplinary piece of work.

During the site visit, the panel met with a number of alumni. All of them are very enthusiastic about the programme and its practical use in their profession. This confirms the high scores in the programme evaluations, indicating the programme's contribution to graduates' careers in the field of cyber security. Large organisations, such as Deloitte and the Ministry of Justice and Security, have sent a number of students over the years and have, by now, a de facto internal team of Master Cyber Security graduates who cooperate on cyber security issues and recommend the programme to other colleagues.

Considerations

The panel appreciates the quality of the theses as an indication that the intended learning outcomes are achieved. The theses are generally proof of well-executed research. The language issues are expected to decrease, because the intake procedure now pays more attention to the level of English and academic writing of candidates. Although short theses can be of very good quality, the panel thinks it is advisable to not only define a maximum length in the thesis guidelines, but also a minimum. This will do justice to the amount of work required.

The panel was a little surprised that students may graduate on the basis of a monodisciplinary thesis. The panel agrees that all students have learned to be part of a multidisciplinary environment during the programme, and that a topic may be disciplinary, but still be related to the general topic of the programme. The panel heard from the alumni that supervisors advise them to narrow their scope down. This may make a topic more monodisciplinary than the student originally intended. Nevertheless, the panel feels that here is a missed chance for this multidisciplinary programme. All students ought to include at least a short section to illustrate the multidisciplinary nature of the learning outcomes, e.g. a reflection on ethical aspects in a technical thesis.

Conclusion

The Master of Science in Cyber Security meets standard 4.

General conclusion

The Master of Science in Cyber Security is a unique programme. The intended learning outcomes are a good indication of both the programme's multidisciplinary nature and the master's level. The programme provides an excellent learning environment, with clear educational objectives, interactive teaching and diverse assignments. The staff is well-qualified, motivated and committed to the students. The programme has an adequate system of student assessment and sufficient mechanisms to safeguard its quality. The theses and careers of the graduates persuasively show that they have achieved the intended learning outcomes.

The panel assesses the Master of Science in Cyber Security as 'positive'.

Recommendations

For further improvement of the programme, the panel has formulated the following recommendations. These recommendations do not detract from the panel's positive assessment of the programme.

- state the programme's position in relation to academic and professional standards and frameworks more explicitly, thus clarifying to academia, the professional field, potential students and their employers what it does and does not offer;
- add more technical electives and a study visit abroad;
- encourage more international students to enroll;

- continue the explicit attention to a course's coherence when inviting guest lecturers;
- invite more guest lecturers from the public sector;
- introduce in-class open-book exams, with less emphasis on reproduction and more on application;
- ask (thesis) examiners to motivate their grade by adding text on the assessment form;
- have an examiner other than the main thesis supervisors, e.g. the track coordinator, to guarantee the multidisciplinarity and the consistency of grading within a track;
- introduce the requirement of a minimum length in the thesis guidelines;
- ask students to include at least a short section in their thesis to illustrate the multidisciplinary nature of the learning outcomes.

Overview of the Assessments

Standard	Assessment
Intended Learning outcomes *Standard 1: The intended learning outcomes tie in with the level and orientation of the programme; they are geared to the expectations of the professional field, the discipline, and international requirements*	Meets the standard
Teaching-learning environment *Standard 2: The curriculum, the teaching-learning environment and the quality of the teaching staff enable the incoming students to achieve the intended learning outcomes.*	Meets the standard
Student assessment *Standard 3: The programme has an adequate system of student assessment in place.*	Meets the standard
Achieved learning outcomes *Standard 4: The programme demonstrates that the intended learning outcomes are achieved.*	Meets the standard
Conclusion	**Positive**

Annexes

Annex 1 Programme of the site visit

Date: 16 January 2020

Location: Wijnhaven building, Turfmarkt 99, The Hague

Programme:

8.30 – 8.45	Arrival and welcome
8:45 - 9:30	Management
9.30 – 9.45	Break
9:45 - 10:30	Lecturers
10.30 - 10.45	Break
10:45 - 11:30	Students (including members Educational Committee)
11.30 – 11.45	Break
11.45 – 12.30	Board of Examiners
12.30 – 13.15	Lunch
13:15 - 14:00	Alumni
14.00 – 16.00	Inspection documentation and deliberation panel
16.00 – 16.30	Presentation of initial findings
16.30 – 17.00	Development discussion

Annex 2 Documents reviewed

Before the site visit

- Self-evaluation report including appendices
- Selection of fifteen theses with their assessment forms
- Information on the background of students (2015-2019)
- Minutes of the Board of Examiners (2015-2019)
- Information on Expert Meetings (2015-2019)
- Exams and assignments for a sample of courses:
    - Cyber Risk Management (general, 2017)
    - ICT systems (technical track, 2017)
    - Cyber Risk and the Social Sciences (general, 2018)
    - Cyber Security Governance (governance track, 2018)
    - Technical Measures and Interventions (technical track, 2018)
    - Introduction to Cyber Space (general, 2019)
    - Cyber Security Management in Organisations (governance track, 2019)
    - Technical Aspects of Cyber Security: an Introduction (elective, 2019)

During the site visit

- Handbooks
- Exam papers (student work) for a sample of courses
    - Cyber Risk Management (general, 2017)
    - ICT systems (technical track, 2017)
    - Cyber Risk and the Social Sciences (general, 2018)
    - Cyber Security Governance (governance track, 2018)
    - Technical Measures and Interventions (technical track, 2018)
    - Cyber Security Management in Organisations (governance track, 2019)
    - Technical Aspects of Cyber Security: an Introduction (elective, 2019)
- Online teaching materials of several courses in BlackBoard
- Quality of Education (policy document, July 2017)
- Final report Institutional Quality Assessment Leiden University and NVAO decision (April 2019)

Annex 3 Abbreviations

BTQ	Basic Teaching Qualification
EC	European Credit
HSD	The Hague Security Delta
LEI	Leiden University
LIACS	Leiden Institute for Advanced Computer Science
NVAO	Nederlands-Vlaamse Accreditatie Organisatie
THUAS	The Hague University of Applied Sciences
TUD	Delft University of Technology
UTQ	University Teaching Qualification