NVAO

MASTER OF SCIENCE IN CYBERSECURITY

KU LEUVEN

CONDUCT-TAILORED INITIAL ACCREDITATION • ASSESSMENT REPORT

29 SEPTEMBER 2021

Table of contents

1 Executive summary

This report constitutes the advice of the panel assessing the quality of the Master of Science programme in Cybersecurity at KU Leuven. The new one-year programme is taught in English and offers a broad range of technical subjects in the domain of cybersecurity. The programme will start in September 2022 and is offered at an advanced (master after master) level. The panel judges the quality of the new programme to be strong, an appreciation that applies to all components of the programme. In view of this holistic judgement, the panel issues a positive advice to NVAO.

The very informative self-evaluation report (Blueprint) and the lively discussions on site demonstrate according to the panel that university and programme management have reflected extensively on all components of the new programme. It thinks highly of the rationale for this programme, as well as of the choices that were made on the level, contents and target group of the new programme, which is unique in Flanders. The panel moreover validates the domain-specific and programme-specific learning outcomes. It also welcomes the commitment and involvement of the professional field in the design and implementation of the programme.

The panel noticed a strong link between the profile of the programme and the structure of the curriculum. The five pillars of the curriculum constitute the full breadth of the discipline with students acquiring foundational knowledge on four pillars and in-depth specialisation in two domains. The team of teaching staff is particularly strong, internationally reputed and very passionate about cybersecurity research and education. The new programme can furthermore rely on state-of-the art facilities.

The programme is embedded in existing policies, frameworks and procedures for both assessment and quality assurance. The panel considers that the assessment plans for the new programme are relevant and robust, and ensure that students meet the learning outcomes by the time they graduate. Moreover, the four-year quality assurance cycle of checks and balances allows the contents of individual courses to be adjusted every year to the rapid evolutions in cybersecurity.

In sum, the panel thinks positively of the quality of MSc in Cybersecurity. It considers that the programme is sufficiently developed to start in September 2022. In addition to all positive appreciations, there is room for strengthening the involvement of students. The suggestions do not affect the panel’s positive judgement on the programme quality. The panel advises to:

- encourage international students to join the Programme Committee;
- communicate systematically to students on the follow-up that is given to course evaluation results;
- seek the input and advice from students before a new programme is finalised and validated by the Programme Committee at faculty level.

The Hague, 29 September 2021

On behalf of the expert panel convened to assess the Master of Science in Cybersecurity

Stefan Katzenbeisser (chair)	Mark Delmartino (secretary)

2 Findings and considerations of the panel

The Master of Science in Cybersecurity is the result of a collaboration between two research units at the Faculty of Engineering Science of KU Leuven: COSIC in the Department of Electrical Engineering and DistriNet in the Department of Computer Science. The new one-year programme is due to start in September 2022 and will be offered at an advanced level, using English as the language of instruction. In view of this initial accreditation visit, the programme has produced an information file, called Blueprint+, that provides a comprehensive description of the envisaged master programme in Cybersecurity. Reporting on its findings and considerations, the panel follows the order of topics as they are addressed in the Blueprint: profile and vision, realisation, and assessment.

Profile and vision

Programme profile

The new master programme intends to educate students in developing digital systems, which are secure against adversarial entities. Students are not only introduced to the different technical areas that underpin security but also learn about social-technical aspects of cybersecurity including security management and legal / privacy elements. Cybersecurity is a very broad discipline: in addition to treating the technical, legal and managerial basics needed by all cyber professionals, the curriculum is built around five technical pillars of cybersecurity: cryptography, privacy, hardware security, software stems security. These pillars reflect the research strengths of COSIC and DistriNet. The one-year full-time programme targets both international and domestic students who already possess a master’s degree in a relevant domain. Upon graduation, students can opt for an engineering career in the cybersecurity industry to design and implement advanced technical solutions, take up positions in other industries where they integrate cybersecurity solutions, or stay connected with academia and pursue a PhD, which in turn could lead to a research career or the creation of a spin-off company.

The panel noticed from the description in the Blueprint that the new programme has been well thought through, an impression that was confirmed during the discussions on site. The proposed master programme addresses an important and timely subject as industry and society are in need of cyber security experts. The programme profile is comprehensive and demonstrates that the applicants know and understand very well the context of cybersecurity in Belgium, across Europe and globally. The panel considers that the new master programme constitutes an effective attempt to address the growing need for cybersecurity specialists.

Following the discussions on site, the panel acknowledges and supports the choices of the programme developers during the design phase of this Cybersecurity master. The programme focuses on the technical aspects of Cybersecurity. By doing so, the programme addresses the most pressing needs in industry. It comes to no surprise according to the panel that all important research areas are covered in this programme: on the one hand, there is a clear alignment between the key pillars in the curriculum and the available research expertise in the applicant departments; on the other hand the expertise of the individual professors and researchers in COSIC and DistriNet is extensive and widely recognised. In this regard, the panel confirms what was stated in the Blueprint and repeated in several discussion sessions: KU Leuven is one of the few universities that has the expertise to cover all aspects of Cybersecurity.

In keeping with the expertise available at KU Leuven, the degree is not aimed at students wishing to specialise in legal and managerial aspects but these aspects are covered to a level needed by professionals working in the technical side of the subject. The panel applauds the holistic view of the programme: while its focus is clearly on technical issues, the programme also addresses the legal, managerial and ethical dimensions of ICT in general and Cybersecurity in particular. The panel understands the position of the programme that society needs experts who do not only talk about cybersecurity but are also able to implement it. It is convinced that the programme's technical focus with attention to non-technical aspects will deliver graduates who are well-rounded experts in the domain of cybersecurity

The choice for a predominantly technical curriculum impacts on the type of students the programme is targeting: engineers, computer scientists and mathematicians/physicists, the latter with some background in programming. In this regard the panel supports the decision to offer the programme at an advanced level, i.e., to students who already possess a master's degree. This advanced (master after master) level in fact allows the programme to focus entirely on the subject of cybersecurity as students will possess the general skills and aptitude of a master student. Moreover, students will be familiar with basic mathematical notation, undergraduate-level mathematics, the principles of computer science, and know how to programme through their initial bachelor and master degrees.

The choice for an advanced master level allows KU Leuven to channel its (research) expertise in Cybersecurity in a one-year full-time specialist programme. Both national and international students informed the panel that they consider it feasible to (come to Leuven and) enrol for a one-year specialist programme that builds upon their initial bachelor and master degrees. The panel therefore understands and supports the choice of the management to design a one-year dedicated cybersecurity programme rather than offering Cybersecurity as a specialist track in the regular initial two-year master programme in Electrical Engineering and/or Computer Science.

Target group

The new programme targets both international students and master students from Belgian universities. The panel understood from the discussions that the programme is not catering exclusively for the Belgian market, but has a distinctly European if not global outlook; hence the importance of targeting not only local but also international students. Currently, there are already many international students in the initial master programmes and these students are equally keen as their Belgian colleagues to enrol in the new programme. Moreover, international students may want to continue their career in Belgium thereby bringing the much-needed expertise in Cybersecurity to Belgium-based companies. Representatives from the professional field also advocated for a combination of domestic and international students in the programme, a choice the panel wholeheartedly underwrites.

According to the programme management, it is the intention to attract yearly between 40 and 50 students. As it is very likely that many more students will show interest in the programme, the developers have elaborated clear admission criteria and a selection procedure. The panel understood from the discussions that the programme prefers quality over quantity, that it wants to attract high quality students and that students who fulfil the admission criteria will be screened extensively. While programme management is ultimately responsible for student intake, it can rely on experienced support from admission services at both central and faculty level. Moreover, the departments and faculty have extensive experience with international students and diverse backgrounds through other initial and advanced master programmes. In addition, one of the envisaged professors in the new programme has long-standing expertise with admissions in both the US and at KU Leuven. The panel supports the applicants' choice for a specialist programme with high quality students and considers that the robust admission and selection procedure ensures that good quality students will eventually enrol.

Educational vision

The panel gathered from the materials that the new programme is fully aligned with the educational vision of the KU Leuven and the Faculty of Engineering Science. In line with this vision, the programme values both breadth and depth of knowledge and aims at expanding the reasoning, communication and problem-solving abilities of students in order to prepare graduates for life-long learning. Moreover, the programme aims at instructing and training students on state-of-the-art knowledge and techniques in cybersecurity. Cybersecurity is an interdisciplinary field: the focus of the programme is on technical aspects, yet the non-technical aspects are addressed, as well. The panel appreciates that the programme not only introduces students to the concepts, methods and tools in the domain of cybersecurity but also provides them a critical and scientific position towards societal aspects (ethics, law, governance) of cybersecurity, and instils an attitude towards life long learning.

Learning outcomes

The educational vision of the university and the profile and ambitions of the programme have been taken on board when translating the programme objectives into learning outcomes. These learning outcomes are listed in annex 2 to this report. Because the proposed programme is new and unique in Flanders, the institution defined independently the domain-specific learning outcomes. The formulation of these learning outcomes was inspired by CyBoK, the Cybersecurity Body of Knowledge, which has been developed in the UK to inform and underpin education and professional training for the cyber security sector. CyBoK defines 19 knowledge areas: the domain-specific learning outcomes cover the majority of these areas. A draft version of the learning outcomes was submitted to the Flemish Council of Universities and University Colleges (VLUHR), which in turn organised a review by employer representatives, internal experts and (former) students of similar disciplines. The panel has studied the learning outcomes. Considering that they are relevant for a master programme in Cybersecurity, the panel validates the set of 11 domain-specific learning outcomes.

The domain-specific learning outcomes have been concretised in 26 programme-specific learning outcomes, which reflect both the domain-specific learning outcomes and the particular profile of the programme. Their formulation and organisation have been influenced by domain-specific reference frameworks the university is using to align its programmes in the respective engineering disciplines. In this case, 26 learning outcomes are structured along seven groups which refer to the learning areas defined by the European standards and guidelines for the accreditation of engineering programmes (EUR-ACE). The panel noticed furthermore that the programme-specific learning outcomes reflect the attention to the five technical pillars of cybersecurity in the programme, as well as the emphasis on research, scientific methodology and the broader societal context of cybersecurity. According to the panel, there is a clear link between the domain-specific and programme-specific learning outcomes, as well as between the programme-specific learning outcomes and the envisaged programme. Both formulated domain-specific and programme-specific learning outcomes are clear, concise and understandable. The panel considers that the programme-specific learning outcomes are formulated in such a way that they do justice to the discipline (cybersecurity), level (master) and orientation (academic) of the programme.

Professional field

The panel noticed that there is considerable interest in the programme from both authorities and professional field. In fact, the new programme is part of a wider government initiative to enhance cybersecurity in Flanders. The concept of the new programme was presented to and discussed with relevant stakeholders in the framework of strategic research agenda meetings on the Cybersecurity Initiative Flanders. During the final development phase, a questionnaire was sent to industry partners to ask for feedback and validation. Moreover, eighteen public and private stakeholders from industry, business and the cybersecurity sector confirmed their interest in the MSc in Cybersecurity by sending a letter of support.

The panel acknowledges these support letters, which confirm the interest of industry and business in – and the urgent need for – this programme. Moreover, the panel gathered from the very interesting discussion on site with eight representatives of the professional field that they fully support the way the programme has been developed and are eagerly awaiting the first graduates. Finally, the panel noticed that the link with the professional field will be maintained once the programme is rolled out, and this in different ways: through a structural dialogue in Industrial Advisory Councils, through a continuation of the many existing informal encounters with the professional field, and by employers (and alumni) feeding back to the programme about the competences of the newly recruited graduates. The panel considers that the involvement of the professional field with the research units, departments and faculty has been strong, that these numerous and regular contacts have helped programme developers in designing a strong and relevant master programme in Cybersecurity, and that this involvement - both structurally and informally - will continue once the programme is up and running.

Realisation

Programme structure

The new MSc in Cybersecurity is offered as a full-time one-year programme where students take compulsory and optional courses and produce a thesis; all together the study load amounts to 60 ECTS. The panel noticed in the informative description in the Blueprint that the structure of the new master programme aligns neatly with its profile. The core components of the programme cover not only a broad range of technical know-how and skills in cybersecurity, but also provide the necessary background in legal and cybersecurity management. The programme is built around five pillars: cryptography, privacy, hardware security, engineering secure software, and software and systems security. The objectives of the five pillars and their respective course contents were described extensively in the Blueprint and further clarified during the discussions on site. The panel thinks highly of the comprehensiveness of the descriptions and the passion with which developers and teaching staff presented the programme as a whole and their courses in particular.

The first semester of the curriculum consists of an introductory programme, fundamental courses in four of the five tracks, and a seminar in cybersecurity that runs for the entire year. During the second semester, students follow in-depth courses on two pillars of their choice, attend courses on security management and the legal and regulatory aspects of cybersecurity, and produce a master thesis. It is an explicit choice of the developers that students on the one hand do not have to focus on every pillar; this allows for a broader intake of students who can drop one domain with which they are less familiar based on their previous education. On the other hand, the developers emphasised that there is enough to learn for students who already possess a particular expertise: they either choose different tracks or customise the contents of their track of expertise with the teaching staff. The panel considers that the value added of the programme lays both in the combination of the five pillars and in the freedom for students to select fundamental and in-depth courses within a selection of pillars. In this regard, the panel sympathises with the statement during one of the sessions that the programme consists of cybersecurity courses worth 90 ECTS of which students choose 60 ECTS.

Curriculum

The panel thinks that the curriculum looks good. It consists of a mixture of new courses that are developed for the purpose of the new programme and existing courses which will be finetuned to welcome the new group of advanced master students. The panel learned from the discussions with teaching staff and students that at KU Leuven, students in initial two-year master programmes (electronical engineering, computer science, mathematical engineering) can take a number of (optional) courses in the domain of cybersecurity, but that this package never exceeds 15 ECTS. At best, these students graduate with expertise in one pillar. According to the panel, this mixture of existing and new courses will also help students with a degree from KU Leuven to decide whether or not to apply for the new MSc in Cybersecurity and tailor their study plan accordingly. In the discussion, KU Leuven students confirmed that the new programme constitutes a relevant option to take into consideration when planning their future academic and/or professional career.

In terms of individual course components and teaching formats, the panel thinks that the set-up of the introductory week - which consists of one week of common introductions to cybersecurity and the programme pillars, and two weeks of project work - is sensible as it provides insight in both the discipline and the study programme and will help students make informed decisions on their individual study plan. Furthermore, the panel understood that the curriculum is quite packed and therefore only allows for a master thesis of 15 ECTS. In order to have students perform in-depth research for a good quality thesis, the programme has reduced the requirements regarding thesis length and set clear deadlines during the thesis trajectory for delivering initial, mid-term and final versions of the thesis. Moreover, students cannot undertake a placement as a dedicated part of the curriculum. Following the discussions on site, the panel agrees to the choices of the programme developers and welcomes the opportunity for students to produce a master thesis in cooperation with industry and spend part of their thesis trajectory in a company.

Teaching formats

The panel also noticed that across the curriculum, courses feature different teaching formats. For instance, several courses dealing with technical aspects will be also conducted as laboratories. The panel also welcomes the use of the flipped classroom approach, as well as the attention for interactive exercises during individual lessons. Moreover, oral and written communication skills – presentations, papers - are trained in the courses and demonstrated at end level in the master thesis and defence. Overall, the pedagogical / educational underpinning of the programme looks good and ensures according to the panel that the courses do not only focus on cybersecurity knowledge transfer and application of know-how and skills in this domain, but also pay attention to communication, and lifelong learning skills.

Alignment between programme and learning outcomes
Further to its statement that the programme profile is translated adequately in the curriculum, the panel gathered from the extensive descriptions in the Blueprint and the discussions on site that there is indeed a strong alignment between the programme learning outcomes and the respective courses in the curriculum. The mapping in the Blueprint between programme-specific learning outcomes and courses demonstrates according to the panel that all learning outcomes are addressed at several parts of the curriculum and that each course aims to train students to achieve several of these learning outcomes.

Teaching staff
The new programme features a core team of lecturers: 12 professors from the COSIC and DistriNet research groups have been closely involved in the design of the programme and are committed to coordinating and delivering the courses assigned to them. The legal aspects of the programme will be covered by a professor from the KU Leuven Centre for IT and IP Law. The panel is aware of the strong academic reputation of these professors and/or noticed from their CVs that they have an extensive research background in specific domains of cybersecurity. This point was also nicely illustrated during the session with students: asked why a foreign student should come to Leuven for this programme, students immediately referred to the expertise of the lecturers, the combination of breadth and depth in Cybersecurity expertise that is available in the two research groups / departments that constitute the backbone of this new programme. The panel fully agrees on this appreciation and considers that the attractiveness of the programme lays among others in its lecturers: the team consists invariably of internationally recognised researchers with a strong publication output and a broad international network. Moreover, the panel spoke to most professors of the envisaged core team and noticed that they are passionate about their research domain and look forward to passing on their expertise to advanced master students in the new programme.

Furthermore, the panel understood from the Blueprint and the discussions that the envisaged teaching staff all had training in didactics and in the pedagogy of teaching, and regularly participate in teaching-related continuing education programmes organised by the Faculty of Engineering Science. The members of the core team also participate in the Cybersecurity Initiative Flanders, which started in 2019 with the goal to support strategic basic research, collaborative research, but also outreach towards industry and professional education. In addition to the core team of envisaged lecturers, the programme can also rely on a big pool of complementary expertise. In addition, the university has a significant number of highly qualified and permanently appointed senior researchers, ‘research managers’ or ‘research experts’. The panel learned that more than 200 people at KU Leuven are currently working on cybersecurity. Finally, the panel welcomes the initiative of the developers to make use of external industrial experts to teach – with the guidance from academic staff - the two management related courses in the curriculum. Hence, students will also be trained by experts with in-depth real-world expertise. These lecturers will provide students an idea of the practical implementation of technical Cybersecurity topics ‘on the ground’, and make them aware of the reality of cybersecurity from a corporate viewpoint.

Infrastructure and educational equipment
Most of the educational activities in the new programme take place on the Heverlee campus of KU Leuven where the departments of Electrical Engineering and Computer Science are

located. The university in general and the Faculty of Engineering Science in particular offer sufficient space to guarantee that all scheduled activities can effectively take place. In this regard, the university management confirmed that the envisaged intake of 40-50 students will not put an additional burden on the infrastructure on the campus. In order to offer all students a good quality educational experience, the programme management told the panel that it intends to stick to this intake figure.

The panel noticed from the Blueprint and the discussions that the standard infrastructure in terms of computer equipment is available in the departmental teaching laboratories. Moreover, the campus offers all the necessary infrastructure to experiment with hardware and software applications. This infrastructure also includes more expensive and specific equipment that is available in the two research groups and will be utilised in project work and in some of the more advanced classes. During the site visit, the panel was shown around in the hardware security lab of the COSIC research group, which is very well equipped for side-channel analysis. The panel was informed that the DistriNet research group features equipment of a similar quality, such as an embedded systems lab and a research and test platform for deploying scalable security services. In sum, the panel considers that the educational facilities of the new programme are good and that the equipment in the research groups is particularly suited for such advanced master programme.

Student support
The panel learned from the Blueprint that the advanced master students on the new programme can make use of all university- and faculty-wide student services, facilities and counselling. Moreover, the university – in cooperation with its student associations - have developed a specific offer to welcome and integrate international students from both a social and educational point of view. In this regard, also the international students on the MSc in Cybersecurity will be encouraged to follow workshops on study approach, time management, cultural differences, KU Leuven examination regulations or writing a master thesis. The panel considers that the students on the new programme can make use of a broad range of adequate student services, a finding that also holds for students with a functional disability. The panel welcomes in particular the many initiatives – such as the Pangaea Intercultural Meeting Centre - that cater to the needs of international students (arriving) in Leuven

In so far as the specific MSc in Cybersecurity is concerned, the panel appreciates that the introductory programme has the explicit objective to help students make informed decisions on the programme pillars. Based on their individual choice for any combination of four pillars, the courses they follow in these pillars will help students in making further in-depth specialisation choices for two pillars in the second semester. In this regard, the panel welcomes the central role of the programme director who will actively coach students in the development of their individualised study plans. Students who need more personal information or guidance can contact their academic adviser, the faculty student administration or the central student support services.

Information on the study
Based on the information in the Blueprint, the panel established that KU Leuven provides general information on all stages of study on its website. This information includes topics like registration, study paths, exams, diplomas and certificates, as well as the educational vision and policy of the university. The panel welcomes the programme-specific information that is provided online in the detailed descriptions of programme and courses in the programme

catalogue. In this way, students and other interested parties – such as the assessment panel – can find comprehensive and readable information on the programme and the different stages of the curriculum.

Once students are enrolled, they have access to internal information that is available to all members of the university community as well as to personal information on their study programme. This information is provided through Toledo, the KU Leuven online learning environment featuring online course content and communication channels between students and teaching staff. Furthermore, students are given access to the KU Leuven Loket application where they can consult their individual study programme, class schedule and individual examination schedule. It also contains the student's academic progress file. According to the panel, both the online learning environment and the Loket application are very useful instruments for all students, including for the domestic and international students on the new master programme in cybersecurity.

Assessment

General test and assessment framework

The new master programme is part of the organisational and administrative responsibility of the Faculty of Engineering Science and as such adheres to the policies of this faculty with regard to education and assessment. The rules and regulations concerning assessment that will apply to the MSc in Cybersecurity are outlined in the faculty document 'Tests and Assessments'. The faculty in general and its degree programmes in particular emphasise the importance of high quality assessment that is fully embedded in the learning environment. The assessment policy of the faculty is organised around five themes: (i) alignment with programme and learning outcomes, (ii) feedback, (iii) quality assurance, transparency and the ombuds service, (iv) evaluation of master thesis and internships, and (v) the organisation of assessments including special provisions for students with a disability. The panel gathered from the elaborate description in the Blueprint how these themes will be implemented in the new master programme. The panel considers that in terms of assessment, the new programme can rely on a strong and relevant framework that is set at faculty level and aligns with the overall policy at university level.

Concrete realisation

The discussions on site provided the panel with additional clarifications and concrete examples on how the test and assessment framework will be applied in the new programme. In this regard, the panel appreciates the programme's attention to feedback and welcomes the broad mix of evaluation activities and assessment forms in the courses: forthcoming master students in Cybersecurity will be assessed through a combination of written exams, oral exams, lab sessions, papers, presentations, etc. Their active participation in class will also be taken into consideration when deciding on the final grade. The evaluation of the master thesis is organised in line with existing processes in the Faculty of Engineering Science: the thesis assessment is performed by a jury composed of the daily supervisor(s), the promoter and at least two reviewers who were not involved in the process. The grading of the thesis is based on a set of rubrics that address (the degree of autonomy in) the thesis work, the quality of the final deliverable, and the thesis defence. While acknowledging that it can only look at the envisaged assessment plans of the new programme, the panel considers that the assessment process is comprehensive and more than sufficiently elaborated to issue a positive opinion at this stage of initial accreditation.

The final objective of the evaluation is to determine whether students eventually achieve the learning outcomes of the programme. In order to verify this for each individual student who is about to graduate, the Faculty of Engineering Science appoints an Examination Committee that is composed of a chair, a secretary, one examiner form each master programme and the ombudsperson. The panel considers this a relevant approach to ensure that students meet the learning outcomes by the time of their graduation.

Quality assurance

While lecturers are responsible for a valid and reliable assessment of their respective courses, it is up to the Programme Committee to monitor the process and outcomes of all assessments within a given programme. Meeting once per month, the Programme Committee consists of the programme director and a delegation of lecturers, teaching assistants and students. The panel learned during the sessions that the Programme Committee is an important instrument for assuring the quality of both education and assessment. The panel was satisfied to hear during the session with students that the Programme Committee is an important and structural body for students to speak out – and be heard – on the quality of education and assessment in the overall programme and the individual courses. Furthermore, the programme management indicated that students who want to assume responsibility in the Programme Committee are offered training. The panel considers the Programme Committee is an effective instrument to monitor education and assessment quality. According to the panel it will be important in the new one-year master programme to ensure that also international students are encouraged to sit on the Programme Committee.

After every course, students are asked to complete a course evaluation covering the quality of education, the competences of the lecturer(s) and the relevance of the assessment. This evaluation is reviewed in the Programme Committee and if necessary, remediation is prescribed. Students indicated to the panel that it is not always clear which follow-up is given to the results from course evaluations. The panel therefore invites the programme management to look for ways in which such follow-up can be communicated systematically in the new programme in Cybersecurity. According to the panel, this is all the more important given the limited duration of the new programme, its multinational composition and its ambition to aim for quality.

Furthermore, the panel noticed that the programme designers did not seek input or advice from students during the development phase. The new programme plans have been presented to (the student delegation in) the Programme Committee at faculty level, but were not shared with the broader group students whose (initial master) programmes would give access to the MSc in Cybersecurity. Hence, the panel's suggestion to look systematically for input and advice from students before programme profiles are finalised.

Public information on programme quality

The panel read in the Blueprint that information on the quality of all programmes at KU Leuven can be consulted in the programme catalogue, which can be consulted by the general public. For the master in cybersecurity this information will be available under the tab 'educational quality' in the programme description in the catalogue. The quality assurance method at KU Leuven is called COBRA, which stands for Cooperation, Reflection and Action and pays attention to the Checks & Balances. The internal quality assurance cycle of a programme lasts four years. At the end of such cycle, the programme reflects on the achieved educational quality, based on qualitative and quantitative input by internal and external actors. The panel got confirmation during the discussions that this formal four-year internal quality assurance cycle does not prevent individual professors and course coordinators to adjust the contents of their courses to new technological evolutions in the domain of cybersecurity. Several interlocuters assured the panel that such adjustments follow their own cycle and rationale and can be implemented every academic year. Acknowledging that it can not yet assess the way the quality assurance tools are operationalised in the new programme, the panel does consider that the university has established a strong engagement for quality assurance that is extensively described on their website. Moreover, the panel is confident that the existing system provides relevant instruments to monitor the quality of the new programme.

3 Assessment

The panel assessing the Master of Science in Cybersecurity at KU Leuven judges the overall quality of the new programme to be good. The appreciation of the panel applies to the profile and vision, realisation, and assessment of the programme. In view of this holistic judgement, the panel issues a positive advice to NVAO.

The very informative self-evaluation report (Blueprint) and the lively discussions on site demonstrate that university and programme management have reflected extensively on all components of the new programme. In terms of profile and vision, the panel acknowledges the link between the profile of the programme and the wider educational vision of the university. It thinks highly of the rationale for this programme, as well as of the choices developers made when profiling the level, contents and target group of the programme. Its unique character is likely to attract many applicants; according to the panel, the admission and selection procedure is sufficiently robust to identify a restricted number of high quality domestic and international students. Furthermore, the panel validates the set of 11 domain-specific learning outcomes and 26 programme-specific learning outcomes as they do justice do the discipline (cybersecurity), level (master) and orientation (academic) of the programme. Another strong feature is the commitment of the professional field to the new programme and their (envisaged) involvement in the preparation and implementation of the curriculum.

In terms of realisation, the panel thinks highly of the rationale for the programme structure and the curriculum: the programme covers the full breadth of the discipline and allows students to not only obtain a basic grounding in the fundamentals of cybersecurity but also an in-depth understanding of two specific domains. Moreover, the teaching staff strongly contributes to the attractiveness of the programme: the team consists of internationally recognised researchers who combine a strong publication output with a broad international network and a passion for cybersecurity education. Finally, the panel established that the educational and research facilities of the new programme are good and that new students can rely on a broad range of services, including specific initiatives for international students.

In terms of assessment, the new programme is embedded in a strong and relevant framework that is set at faculty level and aligns with the overall policy at university level. According to the panel, the assessment plans and processes envisaged for the new programme are both relevant and robust, and ensure that students meet the learning outcomes by the time they graduate. Moreover, the new programme will be integrated in university-wide quality assurance policies and provisions, which are based on a four-year cycle of checks and balances but also allow for yearly adjustments of the course contents.

In sum, the panel thinks positively of the quality of MSc in Cybersecurity. It considers that the programme is sufficiently developed to start in September 2022. In addition to all positive appreciations, there is room for strengthening the involvement of students. The suggestions do not affect the panel’s positive judgement on the programme quality. The panel advises to:

- encourage international students to join the Programme Committee;
- communicate systematically to students on the follow-up that is given to course evaluation results;
- seek the input and advice from students before a new programme is finalised and validated by the Programme Committee at faculty level.

4 Review process

The assessment was carried out in line with the ‘Assessment framework programme conduct-tailored accreditation – October 2018’.

The panel prepared itself for the assessment based on the self-assessment report prepared by the programme when applying for initial accreditation. The panel followed the learning path Initial Accreditation-Own Conduct on the trainings platform. Prior to the preparatory meeting each panel member formulated key findings on the programmes, i.e., strengths, points for attention and issues that required further clarification. The secretary compiled these first impressions in a document that served as a basis for discussion during the preparatory panel meeting.

The panel met on 23 August 2021 to prepare for the accreditation visit. During this online meeting, the panel was informed on the assessment framework and the appreciative approach, in addition to the information provided on the learning path. Moreover, the panel discussed the key findings from the document review and listed the questions per session.

The site visit took place in Leuven on 26 August 2021. The panel spoke to representatives of the university management, as well as to the programme developers, envisaged teaching staff, students from related programmes, and the professional field. Using the appreciative approach, the panel has gathered additional information on the different aspects of the programme. During a closed meeting on 26 August 2021 the panel discussed all information obtained and translated it into a holistic judgement. The panel took this conclusion in full independence.

All information obtained led to a draft assessment report that has been sent to all panel members. The feedback from the panel members has been processed. The assessment report adopted by the chairman was submitted to NVAO on 29 September 2021, followed by a 2 weeks term in which KU Leuven could make comments on factual errors.

Annex 1: Administrative data regarding the institution and the programme

Institution	Katholieke Universiteit Leuven
Address, institution website	Oude Markt 13, B-3000 LEUVEN www.kuleuven.be
Status institution	Publicly funded higher education institutions
Programme	Master of Science in Cybersecurity
Level and orientation	Academic Master
(Additional) title	Not applicable
(Parts of) field of study(s)	Engineering
Specialisations	Not applicable
Programme routes	MSc in Electrical Engineering, Computer Science, Mathematics
Locations	Heverlee Campus, Leuven
Teaching language	English
Study load (in credits)	60 ECTS
New training in Flanders	Yes
Connecting options and potential further education	Not applicable

Annex 2: Learning outcomes

Domain-specific learning outcomes

1. Graduates possess advanced knowledge and understanding of offensive and defensive techniques, methods and tools in the space of cybersecurity, and of their relevance and applicability in practice.
2. Graduates possess advanced knowledge and understanding of theories, methods and tools to model processes and systems and apply these to cybersecurity problems.
3. Graduates are able to assess vulnerabilities and threats on systems in order to identify weaknesses and risks and to validate cybersecurity solutions.
4. Graduates have the knowledge and understanding to develop, deploy and manage cybersecurity protection techniques and tools in collaboration with other cybersecurity experts and with ICT professionals.
5. Graduates are able to independently create (analyse, model and design) solutions for complex problems in cybersecurity research or applications, if appropriate by splitting these up in manageable sub-problems and to critically evaluate the results.
6. Graduates have the required knowledge and understanding of cybersecurity techniques and tools to be able to engage in securing digital services in professional areas such as healthcare, financial services, government, manufacturing, logistics; they are able to independently select appropriate technological means and constructively apply them to a problem in cybersecurity.
7. Graduates are able to critically identify novel problems and assess proposed solutions in cybersecurity, in full awareness of the potential and limitations of the state of the art.
8. Graduates are able to formulate research goals, set up trajectories to pursue these goals, execute those trajectories, and critically assess the results at the level of a beginning researcher.
9. Graduates are able to clearly and accurately report on scientific findings in cybersecurity or on advances in its application domains, both in written and in oral form, and are able to critically assess new scientific developments within subdomains of cybersecurity.
10. Graduates have a good understanding of the interdisciplinary (including psychological, sociological and economic), regulatory and international dimensions of cybersecurity, taking into account the constraints of the various aspects of the sectors they will be part of as professionals (e.g. government, healthcare, software industry, banking and insurance, production industry etc.)
11. Graduates are able to act responsibly from an ethical, legal and professional point of view while taking into account the broader economic and societal context.

Programme-specific learning outcomes

A graduate is competent in one or more disciplines of cybersecurity

1. Has advanced knowledge and insights in the following areas of cybersecurity: basics of cryptography, privacy, software security, hardware security, and system security
2. Can apply this knowledge both in offensive and defensive context (protection)
3. Masters the basics of legal, ethical and management aspects of cybersecurity
4. Understands current research directions in cybersecurity
5. Has specialised knowledge in at least two of the following disciplines of cybersecurity: cryptography, privacy, software security, hardware security, and system security
6. Is able to apply, expand, deepen and integrate knowledge from different fields of cybersecurity

A graduate is competent in conducting research in cybersecurity

1. Can gather all the scientific information relating to a complex cybersecurity problem, assess its relevance and process the valuable aspects
2. Can formulate specific cybersecurity research questions
3. Can independently plan and execute different phases of the research process
4. Can critically evaluate research results
5. Engages other disciplines in the research, where needed

A graduate is competent in applying cybersecurity know-how in concrete problem settings

1. Is able to select cybersecurity technologies in order to protect digital products and services, and to assess the resulting security posture of a specific system or service – for example in professional areas such as healthcare, financial services, government, etc.
2. Can make an informed decision about whether to (re)use an existing security solution based on its properties
3. Can create cybersecurity solutions for open-ended problems and applications

A graduate applies a scientific approach

1. Can critically examine existing concepts, theories, models or interpretations in the field of cybersecurity
2. Identifies and understands the limitations and boundaries of cybersecurity solutions
3. Demonstrates academic integrity in thought and action
4. Is able to independently keep up with developments in the cybersecurity field

A graduate has basic intellectual skills

1. Can rationally cope with different types of information, also with incomplete or irrelevant information
2. Can independently reflect critically and constructively on their own thinking, decision-making and actions
3. Has a critical and constructive approach to developments in the field

A graduate is competent in co-operating and communicating

1. Can orally and in writing communicate about and report on cybersecurity research and solutions in English with laymen, and with specialists and other stakeholders
2. Can efficiently work in groups on a project basis and carry different team roles, can collaborate with professionals from related disciplines

A graduate takes account of the temporal and societal context

1. Takes into account the constraints and the different aspects of the sectors that cybersecurity professionals will be part of (e.g. industry, banking and insurance, healthcare, government, etc.)
2. Is aware of their social and ethical responsibility and acts accordingly
3. Has insight in the broader context of cybersecurity in society (legal, ethical, economic, sociological, psychological and technical-industrial context)

Annex 3: Composition of the panel

The assessment was made by a panel of experts convened and appointed by the NVAO. The panel is composed as follows:

Stefan Katzenbeisser (chair), Professor and Chair of Computer Engineering at the University of Passau (Germany);

Erik Poll (panel member)**,** Associate Professor in Digital Security at Radboud University Nijmegen (Netherlands);

Phédra Clouner (panel member)**,** Deputy Director at the Centre for Cybersecurity Belgium;

Adrian Korzeniowski (student panel member), Master student in Computer Science at the Lodz University of Technology (Poland).

The panel was assisted by:

- **Mark Frederiks**, policy advisor Flanders NVAO, process coordinator;
- **Mark Delmartino,** secretary.

All panel members and the process coordinator/secretary have signed NVAO's code of deontology.

Annex 4: Schedule of the site visit

Thursday 26 August
Campus Heverlee, Kasteel Arenbergpark
Boardroom ESAT-building

Time	Meeting
08.30	Arrival and internal meeting panel
09.00	Session 1 – Representation of the university management
09.45	Session 2 – Programme management (designers curriculum)
11.00	Visit to the COSIC Security Evaluations Lab
11.30	Session 3 – Teaching staff
12.30	Lunch and internal panel meeting
13.30	Session 4 – Students
14.10	Session 5 – Professional field
14.45	Final meeting panel
15.40	Concluding dialogue

Annex 5: Overview of the material studied

Information file

- Self-Evaluation Report Master of Science in Cybersecurity. Initial accreditation. KU Leuven

Annexes to the information file

- Domain-specific learning outcomes
- Corresponding programmes in Flanders and neighbouring countries
- Schematic overview of the entire curriculum
- Description of the content of the curriculum components
- Description of staff and their CVs
- Overview of the contacts with and support letters from the professional field
- Comprehensive and readable information on all stages of study
- Public information on the quality of the programme
- Involvement of internal and external stakeholders, external and independent peers and experts

Documents made available during or leading up to the dialogue

- Application file (and positive result) *Macrodoelmatigheidstoets*
- Information available on the MSc in Cybersecurity on KU Leuven website
- A sample of recent master and PhD theses in the field of cybersecurity
- KU Leuven policy and regulations documents
- Master of Cybersecurity thesis procedures

Colofon

MSc in cybersecurity
KU Leuven (VL131117-21)
Conduct-tailored initial accreditation • Assessment report
29 September 2021
Composition: NVAO • Vlaanderen

NVAO

Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 • 2514 JG Den Haag
P.O. Box 85498 • 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net