NVAO • NEDERLAND

TOETS NIEUWE OPLEIDING

WO-BACHELOR

B CYBERSECURITY & CYBERCRIME

Universiteit Leiden

BEKNOPT ADVIESRAPPORT

9 APRIL 2024

1 Kwaliteitstoets

De toets nieuwe opleiding is een kwaliteitstoets. Een procedure toets nieuwe opleiding (TNO) is een *plan*beoordeling. Een panel van deskundigen toets de kwaliteit van de nieuwe opleiding tijdens een locatiebezoek aan de universiteit of hogeschool. Een discussie tussen 'peers' vormt de basis van de beoordeling en resulteert in een adviesrapport. De inhoud van de opleiding, de toetsing en de studeerbaarheid komen expliciet aan de orde.

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) neemt een accreditatiebesluit op basis van het paneladvies. Dit besluit kan positief, positief onder voorwaarden of negatief zijn. Als het besluit positief of positief onder voorwaarden is, mag de nieuwe opleiding starten. De instelling heeft daarmee het recht om een wettelijk erkend diploma af te geven aan studenten die de opleiding voltooien.

Dit beknopte adviesrapport bevat de belangrijkste uitkomsten van de toetsing door het panel. Een volledig adviesrapport met de bevindingen en overwegingen van het panel is ook beschikbaar. Op basis van het volledige rapport neemt de NVAO een accreditatiebesluit. De NVAO publiceert beide rapporten op haar website.[1]

Meer informatie over de NVAO-werkwijze en de TNO-procedure is te vinden op www.nvao.net.

2 Panel Samenstelling

Prof. dr. Sally Wyatt (voorzitter), Professor Digitale Culturen en decaan voor Onderzoek, Faculty of Arts & Social Sciences, Universiteit Maastricht;
Drs. Liesbeth Holterman (lid), Strategisch adviseur cybersecurity vraagstukken (Konega);
Prof. dr. Albert J. Meijer (lid), Hoogleraar Publiek Management, Universiteit Utrecht;
Ismaïl Sarti (student-lid), student wo-bachelor Wiskunde en wo-bachelor Natuur en Sterrenkunde, Universiteit Utrecht.

Ondersteuning
Marianne van der Weiden (secretaris)
Yvonne Overdevest (NVAO beleidsmedewerker en procescoördinator)

Locatiebezoek
Den Haag, 2 april 2024

[1] https://www.nvao.net/nl/besluiten

3 Oordeel

Het NVAO-panel oordeelt positief over de kwaliteit van de bacheloropleiding Cybersecurity & Cybercrime van de Universiteit Leiden. Studenten volgen een driejarige voltijdsopleiding (180 EC) in Den Haag. De Nederlandstalige multidisciplinaire opleiding leert studenten uitdagingen op het gebied van cybersecurity en cybercrime te identificeren, analyseren en adresseren vanuit technische, juridische en sociaal-organisatorische perspectieven.

De bacheloropleiding Cybersecurity & Cybercrime heeft een uniek en onderscheidend profiel doordat studenten leren het hele proces van cybersecurity te overzien: van preventieve maatregelen (vooraf) tot hoe te reageren achteraf (crisissituatie) en alles daartussen. Ook komt niet alleen de weerbaarheidskant aan de orde, maar ook juist wie de actoren zijn die aanvallen uitvoeren. Studenten leren deze situaties te analyseren en in elke fase passende maatregelen te treffen. Hiervoor is een multidisciplinaire aanpak nodig. Bij cybersecurity en cybercrime gaat het niet alleen om een technisch probleem, maar zijn ook kennis en vaardigheden nodig uit bestuurskunde, recht en criminologie. Zowel overheidsorganisaties als bedrijven hebben grote behoefte aan afgestudeerden van deze opleiding, en het is ook goed mogelijk na afronding door te stromen naar verschillende masteropleidingen.

Om de brede leerdoelen te behalen krijgen studenten vakken in informatica, bestuurskunde, criminologie en recht en ontwikkelen ze professionele en wetenschappelijke vaardigheden. In integratievakken leren ze de verschillende invalshoeken aan de hand van een thema te combineren. De docenten gebruiken creatieve en activerende onderwijsvormen, zoals simulaties, hackathons en *serious games*. De eerste helft van het derde jaar biedt keuzemogelijkheden, zoals een minor, stage of een studieverblijf in het buitenland. Studenten kunnen deze keuzeruimte gebruiken om zich aanvullend in een vak te verdiepen en zo te voldoen aan de ingangseisen van een bepaalde masteropleiding die ze willen volgen. Studenten sluiten de opleiding af met een individueel bachelorondersoek waarin ze twee van de vier vakgebieden combineren. Over de uitkomsten schrijven ze een wetenschappelijk artikel en presenteren ze een poster op een symposium.

De docenten zijn ervaren onderzoekers met veel onderwijservaring. Bij de opleiding zijn vier verschillende instituten betrokken: het Institute of Security and Global Affairs van de faculteit Governance and Global Affairs (penvoerder), het instituut voor Strafrecht & Criminologie en het Centrum voor Recht en Digitale Technologie E-Law van de faculteit der Rechtsgeleerdheid, en het Leiden Institute of Advanced Computer Science van de faculteit Wiskunde en Natuurwetenschappen. Elke faculteit is vertegenwoordigd in het opleidingsbestuur, evenals een student-lid. Zowel het opleidingsmanagement als de docenten overleggen regelmatig met elkaar om de vakken goed op elkaar af te stemmen en piekbelasting te voorkomen. In wekelijkse werkgroepen ontwikkelen de studenten hun vaardigheden, begeleid door een tutor. De tutoren zijn getrainde junior-onderwijskrachten die voor de studenten het eerste aanspreekpunt zijn en een goede schakel vormen tussen de docenten en de studenten. Daarnaast kunnen studenten met vragen of problemen terecht bij de studieadviseur. De opleiding zal beschikken over een eigen onderwijsgebouw in Den Haag waarin studenten en docenten ruimte hebben om samen te werken.

De toetsen om de voortgang van studenten te beoordelen sluiten aan op de leerdoelen van de vakken. De opleiding heeft gekozen voor tussentoetsen om studenten vanaf het begin aan te zetten tot een regelmatig studieritme. Een ervaren en betrokken examencommissie controleert systematisch de kwaliteit van toetsing.

Het panel verwacht dat de bacheloropleiding Cybersecurity & Cybercrime de studenten een boeiende en kwalitatief hoogstaande opleiding zal bieden die goed aansluit bij de behoeften van het werkveld.

4 Sterke punten

Het panel constateert de onderstaande sterke punten:

1. Breed en alomvattend programma – Met de focus op zowel dreigingen als veiligheidsmaatregelen leren studenten het hele proces van digitale onveiligheid en beveiligingsmaatregelen te overzien, van preventie vooraf tot bestraffing achteraf. Studenten leren deze situaties te analyseren en in elke fase passende maatregelen te treffen.

2. Multidisciplinaire aanpak – Om digitale veiligheid in alle aspecten te doorgronden krijgen studenten kennis en vaardigheden uit verschillende vakgebieden: informatica, recht, bestuurskunde en criminologie. Studenten leren kennis uit deze verschillende invalshoeken geïntegreerd toe te passen.

3. Aansluiting op het werkveld – Er is grote behoefte aan afgestudeerden van deze opleiding, zowel in bedrijven als bij de overheid.

4. Innovatieve en creatieve onderwijsmethoden – Docenten gebruiken een variatie aan activerende onderwijsvormen, zoals simulaties, *serious games* en hackathons.

5. Tutoren – Junior-onderwijskrachten begeleiden als tutor de wekelijkse werkgroepen en vormen de schakel tussen studenten en docenten.

5 Aanbevelingen

Met het oog op de verdere ontwikkeling van de opleiding doet het panel een aantal aanbevelingen. Deze aanbevelingen doen geen afbreuk aan het positieve oordeel over de kwaliteit van de opleiding.

1. Aandacht voor ethiek – Maak in de eindtermen van de opleiding expliciet duidelijk dat ethische kwesties die verbonden zijn met cybercrime en cybersecurity – bijv. ethische afwegingen rondom ingrijpende maatregelen – een belangrijk onderdeel van het onderwijs uitmaken.

2. Verticale samenhang – Organiseer een jaarlijks afstemmingsoverleg om te bewaken dat er in elk van de vier disciplines sprake is van systematische kennisopbouw in een doorlopende leerlijn door de verschillende jaren van de bachelor heen.

3. Voorbereiden op groei – Anticipeer op de mogelijk grote toeloop van studenten door tijdig voldoende personeel aan te trekken, de werklast te bewaken en voldoende middelen te reserveren voor bijvoorbeeld extracurriculaire activiteiten.

4. Beoordeling eindproject – Stimuleer zowel creativiteit en innovativiteit als maatschappelijke betrokkenheid en relevantie in het eindproject door deze aspecten op te nemen in de beoordelingscriteria voor het eindwerkstuk.

5. AI en ChatGPT – Blijf alert op ongeoorloofd gebruik van *generative* AI bij toetsen en scherp zo nodig de controlemechanismen en procedures aan.

6 Hoe gaat het verder?

De NVAO neemt een accreditatiebesluit nieuwe opleiding op basis van het volledige adviesrapport van het panel. Dit besluit heeft een geldigheidsduur van zes jaar. Voor een accreditatiebesluit onder voorwaarden gelden andere bepalingen. Na accreditatie valt de nieuwe opleiding onder de gewone accreditatieprocedure voor bestaande opleidingen. De NVAO publiceert het besluit samen met het volledige rapport en deze beknopte versie ervan op haar website.[2]

Het interne systeem van kwaliteitszorg van de universiteit of hogeschool voorziet in passende vervolgacties die verzekeren dat de instelling de eigen visie op goed onderwijs realiseert. Een belangrijke bijdrage leveren de onderwijsvisitaties van opleidingen en diverse tussentijdse ‘peer reviews’. Bij de volgende visitatie zal de opleiding

[2] https://www.nvao.net.nl/besluiten

terugkoppelen over wat zij met de aanbevelingen van het panel heeft gedaan. Deze verbeteracties krijgen ook een plek in het volgende adviesrapport. Meer informatie daarover op de website van de instelling.[3]

7 Summary

The outcome of the initial accreditation of the bachelor programme Cybersecurity & Cybercrime of Leiden University is positive. The Accreditation Organisation of the Netherlands and Flanders (NVAO) organised a peer review and convened a panel of experts who visited the institution in The Hague on 2 April 2024.

The bachelor programme provides students with a thorough basis in informatics, governance, law and criminology, combined with a set of professional and academic skills. This prepares graduates to address issues of cybersecurity and cybercrime in all phases of incidents. The programme is unique for the Netherlands. Representatives of national public and private organisations have been involved since the development phase and welcome the graduates of this new programme.

The curriculum is up to date and comprehensive. Students acquire not only basic knowledge of the four disciplines, but also learn in thematic courses how to integrate these different approaches. They develop skills in critical and ethical thinking, how to do academic research, and practical skills such as programming, oral and written communication skills and working effectively in groups. Teaching methods are innovative and creative, including hackathons, simulations and serious games. In the final year, students write an individual bachelor thesis. Students are guided in their studies by an intensive tutoring programme. The teaching team is of high quality. Coordination between members of the team is strong. Staff and students will be housed in a newly renovated building in the centre of The Hague. This dedicated place is expected to contribute to multidisciplinary cooperation and the community atmosphere, for both staff and students.

Assessments and examinations are well in line with the programme's learning goals. Mid-term assessments are an effective way of stimulating a regular study rhythm and spreading the study load for students. A strong and well-experienced Board of Examiners guarantees the quality of assessment and the level of the degree.

Further information about NVAO and the quality assurance system in the Netherlands can be found on www.nvao.net. For more information on Universiteit Leiden see the university's website.[4]

[3] https://www.universiteitleiden.nl/
[4] https://www.universiteitleiden.nl/en

Het beknopte adviesrapport is tot stand gekomen in opdracht van de NVAO met het oog op de beperkte toetsing van de nieuwe opleiding B Cybersecurity & Cybercrime van de Universiteit Leiden

Aanvraagnummer: AV-2165

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