Reactie op internetconsultatie Cyberbeveiligingswet[1]
namens Universiteiten van Nederland en Vereniging Hogescholen, 1 juli 2024.

De herziene *Network and Information Security* (NIS2) richtlijn van de Europese Unie richt zich op de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten. Met dit wetsvoorstel implementeert Nederland deze Europese NIS2-richtlijn in de nationale wetgeving.

De Europese NIS2-richtlijn schrijft niet voor dat de maatregelen gaan gelden voor onderwijs-instellingen. Bij de beraadslagingen in Europa is pas op het laatste moment in het traject van totstandkoming van de richtlijn de optie toegevoegd om lidstaten – indien zij dit zelf noodzakelijk achten – de mogelijkheid te bieden onderwijsinstellingen toe te voegen aan de essentiële of belangrijke entiteiten. Optioneel dus. De 'kan'-bepaling spitst zich uitdrukkelijk toe op onderwijsinstellingen 'die kritieke onderzoeksactiviteiten verrichten', terwijl uit bijlage 1 bij de duiding van onderzoek als kritische sector, onderwijs expliciet uitgesloten wordt, en in de toelichting blijkt dat het type onderzoek aan universiteiten en hogescholen niet valt onder kritische sectoren. Daarmee vindt aanwijzen van het hoger onderwijs geen grond in de Europese richtlijn of in een Nederlandse vertaling hiervan, maar zou uitsluitend een aanvullende eigen beleidskeuze zijn van de Nederlandse overheid. Het ministerie van OCW heeft hierover nog geen standpunt ingenomen.

UNL en VH willen benadrukken dat er tegen deze achtergronden bezien geen nut of noodzaak is om hogescholen en universiteiten aan te wijzen onder de NIS2-richtlijn. Daarnaast zal het een groot aantal zeer ongewenste gevolgen op de korte termijn hebben die ook de beweging naar een veiligere sector eerder tegenwerkt dan helpt. Dit onderbouwen wij graag met een aantal inzichten en zorgen. Tevens geven we een suggestie voor aanpassing van de Nederlandse wetsteksten met duidingen die in de Europese NIS2-richtlijn worden genoemd maar vooralsnog in de Nederlandse teksten ontbreken.

De NIS2-richtlijn is in het leven geroepen om kritische infrastructuur te beschermen. De universiteiten en hogescholen erkennen volledig het belang hiervan. Hoewel bescherming van kennis en informatie, netwerken en informatiesystemen ook voor onze instellingen van groot belang is en zij daar met het bestaande beleid op kennisveiligheid en cyberweerbaarheid volop aan werken, vallen zij -met reden- niet onder de definitie van kritische infrastructuur blijkens de Europese richtlijn. Aanwijzing is dan ook niet vereist, maar een keuze die de minister kan maken. Als die keuze inderdaad gemaakt zou worden, heeft dat naar onze verwachting een onevenredig grote impact op de sector, terwijl het de vraag is of een aanwijzing wel substantieel meerwaarde zal brengen ten opzichte van de serieuze stappen en resultaten die momenteel al aantoonbaar geboekt worden in informatieveiligheid; en waarvoor alle instellingen zich ook in de toekomst maximaal blijven inspannen.

Maatschappelijke taken hoger onderwijs in relatie tot NIS2
De maatschappelijke taak van universiteiten en hogescholen is het geven van hoogwaardig onderwijs, het verrichten van onderzoek van wereldniveau en het realiseren van maatschappelijke impact, om daarmee te bouwen aan een sterke kennissamenleving. Zo dragen de instellingen bij aan een krachtige samenleving waarmee Nederland internationaal een vooraanstaande positie behaalt en behoudt. De netwerk- en informatiesystemen van hogescholen en universiteiten zijn ingericht om te kunnen voldoen aan deze maatschappelijke taak. De taken en ook de risico's in het hoger onderwijs verschillen echter fundamenteel van die in de kritieke infrastructuren die de NIS2-richtlijn beoogt te beschermen. Cyberaanvallen op hoger-onderwijsinstellingen zijn ongewenst en problematisch, maar zij ontwrichten geen (delen) van de maatschappij en vormen geen acuut risico voor de nationale

[1] Gepubliceerd op: https://www.internetconsultatie.nl/cyberbeveiligingswet/b1

veiligheid. Dat kennis en informatie desalniettemin goed beschermd moet worden, staat hierbij niet ter discussie.

Informatiebeveiliging in het HO: ambities en resultaten
Het belang van informatieveiligheid, cyberweerbaarheid, kennisveiligheid wordt in de HO-sector volledig onderschreven. Er is al veel in geïnvesteerd en deze inspanningen worden krachtig voortgezet. Dit vertaalt zich ook in meetbare resultaten. Aanwijzing onder NIS2 is niet nodig omdat het geen meerwaarde heeft ten opzichte van wat er al gedaan wordt.

Voor informatiebeveiliging en cyberweerbaarheid hanteren alle hoger onderwijsinstellingen een formeel en voor de sector passend toetsingskader, gebaseerd op standaarden van de Internationale Organisatie voor Standaardisatie (ISO). Dit op het hoger onderwijs toegespitste kader, ook wel SURF-normenkader genoemd, is de basis voor periodieke, formele en externe audits. Er is een sectorbreed ambitieniveau vastgesteld en op basis van de audits worden systematische en continue verbeterprocessen gevolgd. Er wordt verantwoording afgelegd in Raden van Toezicht, jaarverslagen en er vindt halfjaarlijks bestuurlijk overleg plaats met het ministerie van OCW over de voortgang.

De HO-sector, veelal via het coöperatief platform van SURF, loopt al vele jaren voorop in deze ontwikkelingen, onder meer door het organiseren van centrale expertise in bijvoorbeeld het gezamenlijke *Computer Emergency Response Team* voor onderwijs en onderzoek (het SURFcert) met daarin securityexperts van aangesloten instellingen en SURF. Ook door verschillende incidenten, zoals de cyberaanval aan de Universiteit Maastricht in 2019, is het bewustzijn van risico's en het belang van weerbaarheid op alle niveaus onverminderd hoog. Met nog steeds groeiende focus investeren instellingen in zowel in technische als organisatorische maatrelen om de digitale weerbaarheid te blijven vergroten en ook toetsbaar te maken. Kortom, cyberveiligheid heeft een hoge prioriteit op de bestuurlijke agenda van alle HO-instellingen, van de sector als geheel en van partners in de samenwerkingsketens. NIS2 zal dat niet verder verbeteren maar eerder de focus van de instellingen noodgedwongen verleggen en bestuurlijke risico-afwegingen een stuk ingewikkelder maken.

Huidige informatiebeveiliging in relatie tot vorm en opbrengst NIS2
De nieuwe NIS2-richtlijn schrijft specifieke vormen van zorgplicht, meldplicht en toezicht voor, die in veel facetten lijken op hetgeen er al in het HO gebeurt, maar de specifieke vormvereisten vergen grote veranderinspanningen ten opzichte van het hele huis aan procedures die op dit moment al in positie en uitvoering zijn, met goede resultaten.

In de huidige situatie zorgen instellingen reeds voor passende beveiligingsmaatregelen, waaronder basismaatregelen zoals multifactor-authenticatie, netwerksegmentering, detectie (d.m.v. SOC/SIEM) en awareness programma's. Zij testen de cyberweerbaarheid periodiek door middel van o.a. zogenaamde Pentests. Informatie over pogingen tot inbreken of andere risico's worden gemeld en gedeeld binnen het hechte netwerk van specialisten via de platforms van SURF. Bij cyberaanvallen biedt SURFcert ondersteuning en advies aan de Incident Respons Teams bij de instellingen. Het SURFcert is onderdeel van het Landelijk Dekkend Stelsel van het Nationaal Cyber Security Centrum (NCSC). Op het gebied van cyberweerbaarheid blijken de getroffen maatregelen grote dreigingen te hebben kunnen afweren. Naast de toegenomen cyberweerbaarheid is dat waarneembaar in de positieve resultaten en trends in de externe audits op dit gebied. Naast de interne toezichtmaatregelen in de instellingen hebben ook Raden van Toezicht het onderwerp hoog op de agenda staan.

Het is de vraag welke meerwaarde andere vormvereisten onder aanwijzing van de wetgeving zullen hebben. De extra inspanningen en investeringen om hieraan te kunnen voldoen zullen echter groot

zijn, niet alleen aan de zijde van de instellingen, maar het zal ook veel vragen van overheid en inspectiedienst. De administratieve lastendruk zal (contrair aan alle goede intenties) toenemen, terwijl alle HO-instellingen deze energie liever steken in het verder brengen van de cyberweerbaarheid zelf, bijvoorbeeld door zowel dit jaar als volgend jaar weer aantoonbare volgende stappen te maken volgens het volwassenheidsmodel voor informatiebeveiliging en kennisveiligheid. Er is veel goede energie in de instellingen op deze onderwerpen en de actuele resultaten worden periodiek gedeeld met het ministerie van OCW.

Verwachte gevolgen NIS2 voor (internationale) samenwerking in onderwijs en onderzoek
Een andere vorm van impact van NIS2 voor het hoger onderwijs en onderzoek is die op het onderwijs en onderzoek. Afhankelijk van de gevolgen van de wetgevingsvereisten kan er verandering nodig zijn in het gebruik van specifieke diensten, systemen of technologie die vereist zijn voor het aanbieden van onderwijs of het samenwerken in onderwijs en onderzoek, passend bij de maatschappelijke taken. Deze impact kan groot zijn als in Nederland de instellingen worden aangewezen voor de NIS2, maar in overige landen niet. In de afgelopen maanden is gebleken dat hier nog geen eenduidig beeld over bestaat. Bijvoorbeeld Duitsland en België zullen de HO-sector vooralsnog niet aanwijzen. Mochten de Nederlandse instellingen op dit moment wél aangewezen worden, dan is de impact op Europese en internationale samenwerking onderwijs en onderzoek ongewis.

HO-instellingen als essentiële of belangrijke entiteiten?
Hoger-onderwijsinstellingen zetten grote stappen op informatiebeveiliging, cyberweerbaarheid en kennisveiligheid om zorg te dragen voor open en veilig onderwijs en onderzoek. Blijkens het concept-wetsvoorstel kunnen bekostigde universiteiten en/of hogescholen op enig moment bij regeling of besluit door de minister van OCW worden aangewezen als essentiële entiteit (artikel 11) of als belangrijke entiteit (artikel 14). De betreffende artikelen noch de memorie van toelichting bevatten criteria voor een dergelijk besluit. Datzelfde geldt voor het afwegingskader wanneer die aanwijzing dan leidt tot een aanwijzing als essentiële of belangrijke entiteit. Ook is opvallend dat en onduidelijk waarom dit dan kennelijk uitsluitend voor bekostigde instellingen zou gelden.
De EU-richtlijn geeft aan (artikel 5b) dat de lidstaten de richtlijn van toepassing kunnen verklaren op onderwijsinstellingen, ‘met name wanneer zij kritieke onderzoeksactiviteiten verrichten’. In de Nederlandse wet ontbreekt deze nadere aanduiding waardoor de beperkende werking van deze aanduiding achterwege blijft. Het zou gegeven alle bovenstaande overwegingen zorgvuldig zijn deze verwijzing naar kritische onderzoeksactiviteiten en daaraan gekoppeld ook uitdrukkelijk de door de EU bedoelde interpretatie van wat kritische onderzoeksactiviteiten zijn, in de Nederlandse wetgeving over te nemen.
Verder zou conform artikel 15 van de EU richtlijn afwegingen moeten plaatsvinden op basis van relevante sectorale risicobeoordelingen waarbij gestreefd wordt naar een billijk evenwicht tussen risicogebaseerde eisen en verplichtingen enerzijds en administratieve lasten die voortvloeien uit inrichting en toezicht op naleving anderzijds. We pleiten tevens voor het opnemen van deze verwijzingen naar sectorale risicobeoordeling en het billijk evenwicht tussen maatregelen en administratieve lasten in de Nederlandse wetgeving.

Concluderend: gezien de grote gevolgen van een besluit tot aanwijzing per AMvB voor de instellingen, de geringe verwachte meerwaarde, en de verschillen in duiding in vergelijking met de Europese richtlijn, zou te zijner tijd aanwijzing op basis van het wetsvoorstel onzorgvuldig en onwenselijk zijn.