MJP Cybersecurity – Digitale Veiligheid en Privacy

1. *Dit bestaande meerjarenprogramma wordt gecontinueerd in 2020-2024 en behoort tot het cluster*: **Digital technologies**.

2. *Welke sleuteltechnologie(ën) staa(t)n centraal:* **Digital security / Encryption technologies**.

3. *Positie NL.*
   Ondanks de geringe omvang van de Nederlandse onderzoeksgemeenschap in data- en systeembeveiliging behoren de wetenschappers uit deze gemeenschap tot de wereldtop. Zij scoorden in de afgelopen drie jaar gemiddeld liefst 10 toppublicaties per jaar in de "top-4" security conferenties (Security & Privacy, CCS, USENIX Security, en NDSS). Verschillende Nederlandse universiteiten staan in de top-100 van de wereld, gemeten naar het aantal publicaties in deze conferenties (waarvan 1 op positie 13), waarbij één van de Nederlandse onderzoekers in de top-20 allertijden staat wat betreft het aantal toppublicaties in deze conferenties. Ook in de twee topconferenties in cryptografie (CRYPTO en EuroCrypt) deden de Nederlandse onderzoeksgroepen het goed met meer dan 7 publicaties per jaar, en met de 15e positie wereldwijd in deze periode. Nederlandse onderzoekers nemen actief deel aan competities van NIST voor nieuwe crypto standaarden, bijvoorbeeld op het gebied van post-quantum crypto en lightweight authenticated encryption and hashing (zie https://csrc.nist.gov/projects/lightweight-cryptography). Nederlandse onderzoekers spelen een grote rol in de organisatie van mondiaal onderzoek, in steering committees, besturen van Europese onderzoeksinstellingen en netwerken op het gebied van cybersecurity. Doordat de investeringen in Nederland achterblijven, is het wel zo dat onze positie onder vuur ligt. Grote onderzoeksinstituten in landen als Duitsland in Europa en de VS in Noord-Amerika nemen afstand, en trekken ook actief onze beste onderzoekers aan. Om de huidige positie tenminste te handhaven is versterking aan de basis (via vaste posities) noodzakelijk. Door de geringe omvang kunnen kleine mutaties grote verschuivingen in impact tot gevolg hebben.

4. *Korte beschrijving van voorgesteld meerjarenprogramma voor onderzoek en ontwikkeling.*
   De *nationale cyber security research agenda* (NCSRA-III) vormt het kader voor het Nederlandse cybersecurity onderzoek. Eén van de grote informatica-uitdagingen waar de discipline voor staat is hoe de (on)veiligheid van een systeem aangetoond kan worden en hoe eventuele kwetsbaarheden automatisch te detecteren en repareren zijn. Daarbij komt dat de funderende principes van het ontwerpen en ontwikkelen van veilige systemen en software nog volstrekt onvoldoende bekend zijn. Maar hoe goed systemen ook ontwikkeld kunnen worden, geanalyseerd op kwetsbaarheden en gerepareerd, er blijft een dringende behoefte aan betere methodes om aanvallen te detecteren en systemen actief te verdedigen. Verder is er de uitdaging hoe privacy in de steeds verder gedigitaliseerde samenleving te garanderen is, terwijl de grenzen van technologische oplossingen nog onduidelijk zijn en wet- en regelgeving noodzakelijk zijn om bescherming af te dwingen. Dit komt met name tot uitdrukking in de noodzaak tot flexibele, veilige en privacy-vriendelijke identity management, niet alleen voor authenticatie, maar ook voor digitale ondertekening, bijvoorbeeld voor het vastleggen van toestemming in het kader van de AVG. Tot slot ligt er een wetenschappelijke, maatschappelijke en economische uitdaging in de opkomst van onveilige Internet of Things (IoT) systemen. Voor de cybersecurity en cyber-privacy van IoT-systemen zijn doorbraken nodig in alle pijlers onder de NCSRA-III (design, defence, attacks, governance en privacy). Concrete wetenschappelijke uitdagingen zijn: een veilige "smart" wereld, ondanks ontelbare onveilige apparaten in het IoT, het automatisch detecteren en verhelpen van kwetsbaarheden en het begrijpen hoe prikkels helpen ter verhoging van de veiligheid. Het in de NCSA en NDS aangekondigde kennisontwikkelingsprogramma is leidraad voor de uitvoering van de NCSRA-III.

5. *Ecosysteem.*
   Het ecosysteem bestaat uit de stakeholders van het Dutch cybersecurity platform voor higher education and research - dcypher: waaronder de oprichters van dcypher - ministeries, NWO, ministeries betrokken bij de cybersecurity NWO programmering, de dcypher Adviesraad, the Hague Security Delta, en de vele publieke - en private instellingen die zijn aangesloten bij dcypher. Gezien de urgentie van de cybersecurity

problematiek zijn reeds een aantal PPS voorstellen ingediend in recente NWO en NWA calls. Indien gefinancierd vormen deze programma's een kiem voor het hier voorgestelde MJP.

6. *Organiserend vermogen*.
   De sector is goed georganiseerd voornamelijk via dcypher, waarin wetenschap, bedrijfsleven en overheid participeren en in het bijzonder gezamenlijke onderzoeksagenda's ontwikkelen. Daarnaast heeft deze sector zichzelf duidelijk op de politieke agenda weten te krijgen vanwege de "brandbrief" van de hoogleraren Bos, Jacobs, van Eeten en de resulterende Kamermotie, op basis waarvan nu door EZK nationaal cybersecurity beleid ontwikkeld wordt. De Nederlandse overheid werkt aan de crypto strategie voor de komende jaren, die opgezet word door het Nationaal Bureau Verbindingsbeveiliging (NBV onderdeel van AIVD), in overleg met de academische community.

7. *Kans op maatschappelijke impact op korte en lange termijn.*
   De sleuteltechnologie cybersecurity draagt vooral bij aan de maatschappelijke uitdaging Veiligheid (waaronder cyber-, defensie- en waterveiligheid). Omdat cybersecurity (inclusief privacy) een sector-doorsnijdend karakter heeft is er ook een hoge mate van verbondenheid met digitalisering binnen de andere drie maatschappelijke thema's.

8. *Kans op economische impact op korte en lange termijn*.
   Binnen de eerste NWA-call is een breed gedragen, groot voorstel ingediend over security en IoT, met massale steun vanuit het bedrijfsleven. Meer in het algemeen heeft het bedrijfsleven grote behoefte aan interactie met de academische wereld, op een niveau dat dicht zit bij de ontwikkelde producten en diensten. De kans op economische impact is zowel op korte als lange termijn erg groot. Het cybersecurity onderzoek in Nederland heeft een track record van impactvolle innovaties, zoals de anti-DDoS werkgroep, die onder leiding van het NCSC is ontstaan, de 4.TU spin-off SecurityMatters en IRMA, de non-profit spin-off van NCSRA funding, via de stichting https://privacybydesign.foundation/.

9. *Krachtenbundeling.*
   De Nederlands onderzoeksgemeenschap heeft goede contacten met de European Union Agency for Network and Information Security (ENISA), de European Cyber Security Organisation (ECSO), H2020 Cybersecurity Competence Centers, het CODE Cybersecurity instituut van de UNIBW in München, het Helmholtz Center for Information Security (CISPA) in Saarbrücken, en met het nieuwe Max Planck instituut voor Cybersecurity in Bochum. Daarbuiten bestaat er een nauwe onderzoekssamenwerking met het Amerikaanse Department of Homeland Security (DHS) en de National Science Foundation (NSF) via gezamenlijk onderzoekscalls met NWO (onder coördinatie van dcypher). Nederland is betrokken bij twee Europese pilots: CONCORDIA en CyberSec4Europe. Deze moeten bijdragen aan een gemeenschappelijke 'European Cybersecurity Research & Innovation Roadmap' voorbij 2020 en aan een 'European cybersecurity strategy for industry'.

10. *Cross-over karakter*.
    De cybersecurity gemeenschap heeft een lange traditie van interdisciplinaire onderzoekscalls, in het bijzonder samen met juridische en sociale wetenschappen. Zulke interdisciplinaire samenwerking krijgt op verschillende locaties concrete vorm, bijvoorbeeld in Nijmegen met een interdisciplinaire hub voor security, privacy en data governance (www.ru.nl/ihub) en de TU Delft socio-tech samenwerking (www.tudelft.nl/cybersecurity).

11. *Benodigde gemiddelde jaarlijkse financiering en commitments voor periode 2020-2024*

Bron	**Totaalbedrag (in mln EUR per jr)**	**Waarvan reeds gecommitteerd**	**Waarvan te mobiliseren**
Private middelen	*4*		*4*
PPS toeslag	*1*		*1*
TO2 middelen	*3*	*2*	*1*
NWO	*6*		*6*
Universiteiten/hogescholen	*3*	*3*	

Regionale middelen (provincie, gemeenten)	*1*		*1*
Departementale middelen	*2*		*2*
EU middelen	*2*		*2*
ROMs en InvestNL			
Anders, namelijk:			
Totaal bedrag	***22***	***5***	***17***