Inbreng Verslag van een schriftelijk overleg

Binnen de vaste commissie voor Digitale Zaken hebben enkele fracties de behoefte om enkele vragen en opmerkingen voor te leggen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over de brief d.d. 17 mei 2024 inzake ‘Fiche: Aanbeveling Routekaart Post-Quantumcryptografie’ (Kamerstuk 22112, nr. 3945).

De fungerend voorzitter van de commissie,
Kathmann

Adjunct-griffier van de commissie,
Muller

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie
Vragen en opmerkingen van de leden van de VVD-fractie
Vragen en opmerkingen van de leden van de NSC-fractie

II Antwoord / Reactie van de bewindspersoon

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van het Fiche Aanbeveling Routekaart Post-Quantumcryptografie. Deze leden erkennen het belang van cryptografisch veilige communicatie binnen het digitale domein voor de samenleving als geheel en de uitdagingen die quantum computing met zich meebrengt voor traditionele manieren van asymmetrische cryptografie. Deze leden juichen het dan ook toe dat zowel de Europese Commissie als de minister zich inzet voor technologieën die ook in een post-quantum wereld nog bestand zijn tegen kraken. Wel hebben de leden van de GroenLinks-PvdA-fractie enkele vragen en opmerkingen over het fiche.

2. Essentie voorstel

De leden van de GroenLinks-PvdA-fractie juichen het toe dat de Europese Commissie lidstaten aanraadt om reeds na te denken over een post-quantum wereld. Deze leden zijn benieuwd naar de juridische en praktische gevolgen van een Routekaart Post-Quantum Cryptografie waar de Europese Commissie op aanstuurt. Kan de minister aangeven wat een dergelijke routekaart in de praktijk zal betekenen? Kan Nederland eigenstandig andere mogelijke technologieën onderzoeken die in een post-quantum wereld cryptografisch van nut zouden kunnen zijn indien die niet in de routekaart zijn opgenomen? Kan de minister aangeven hoe zij een dergelijke routekaart waardeert?

Daarnaast zijn de leden van de GroenLinks-PvdA-fractie van mening dat Europese samenwerking op het gebied van post-quantum cryptografie zeer nuttig kan zijn. Deze leden zijn dan ook verheugd dat de Europese Commissie oproept om de acties te coördineren via een op te richting toegewijd lidstatenforum. Tegelijk is Nederland lid van de Appropriately Qualified Authorities (AQUA) Reference Group. Kan de minister aangeven hoe zij dit op te richten toegewijd lidstatenforum waardeert ten opzichte van de AQUA Reference Group? Is Nederland voorstander van een op te richten lidstatenforum? Is zij van plan om toe te treden tot het lidstatenforum en blijft Nederland in dat geval óók lid van de AQUA Reference Group? Welke rol ziet zij daarin voor Nederland weggelegd? Hoe beoordeelt zij de overeenkomsten en verschillen tussen beiden gremia?

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

De leden van de GroenLinks-PvdA-fractie vinden het prettig dat reeds in 2021 is begonnen met het Rijksbrede programma Quantumveilige Cryptografie Rijk en dat er sinds 2014 aandacht is voor de dreiging van de quantumcomputer. In dat kader zijn deze leden benieuwd naar hoe de minister kijkt naar de *store now decrypt later* problematiek, waarin datasets die eerder verzameld zijn op een later moment nog door een krachtige computer worden ontsleuteld. Welke risico's brengt deze problematiek met zich mee, hoe kunnen deze worden gemitigeerd?

b) Beoordeling + inzet ten aanzien van dit voorstel

De leden van de GroenLinks-PvdA-fractie delen de positieve houding van het kabinet ten aanzien van de voorgestelde acties uit de aanbeveling van de Commissie om de transitie EU-breed aan te pakken. Deze leden zijn echter wel verrast over de kritiekpunten van het kabinet op het voorstel van de Commissie. Zij snappen de keuze van de Commissie om zowel post-quantum cryptografie (PQC) als quantum key distribution (QKD) onder hybride constructies te verstaan. Kan de minister aangeven waarom zij dit anders ziet? Wat is het risico als QKD ook wordt opgenomen in de Europese routekaart? Wat zijn de voor- en nadelen van het investeren in QKD *naast* PQC?

De leden van de GroenLinks-PvdA-fractie snappen dat QKD zich nog in een ontwikkelfase bevindt en dat PQC al verder ontwikkeld is, waarbij QKD tevens praktische bezwaren kent als dure en weinig beschikbare benodigde hardware. Deze leden zijn echter vooral benieuwd naar de redenen om QKD als technologie op voorhand af te wijzen, waarbij op dit moment nog niet duidelijk is of de use-case van QKD naast PQC wél van nut kan zijn in de toekomst. Deelt het kabinet de visie dat praktische bezwaren van QKD die er op korte termijn zijn, op langere termijn wellicht wél weggenomen kunnen worden? Waarom zou QKD niet genoemd kunnen worden in de aanbeveling als de EU hier samen met lidstaten wel in investeert, onder andere in het kader van de European Quantum Communication Infrastructure? Welke lidstaten delen de visie van de inlichtingendiensten van Nederland, Frankrijk, Duitsland en Zweden t.a.v. het niet opnemen van QKD in de aanbeveling en in de gezamenlijke Europese Routekaart en welke niet? Welke redenen geven de lidstaten die wél voorstander zijn van het opnemen van QKD in de aanbeveling? Ondersteunt het kabinet op dit moment onderzoeksprojecten op het gebied van de praktische toepassing van QKD? Zo ja, welke projecten zijn dat? Zo nee, welke praktische, inhoudelijke en principiële redenen liggen daaraan ten grondslag? Wat is een mogelijk nadeel als de EU – in navolging van de wens van Nederland – in dit stadium nog niet inzet op QKD en andere grootmachten wel? Kan de minister in de breedste zin van het woord op reflecteren op bovenstaande vragen?

Daarnaast snappen de leden van de GroenLinks-PvdA-fractie de wens van het kabinet tot het volgen van standaardisatieorganisaties zoals de ISO, NIST, en IETF. Deze leden hebben hier echter nog wel enkele vragen over. Ten eerste vragen zij hoe het kabinet de invloed van andere geopolitieke grootmachten binnen dergelijke standaardisatieorganisaties beoordeeld. Hoe ziet het kabinet de relatieve invloed van grootmachten als de Verenigde Staten, de Europese Unie, China en anderen binnen dergelijke standaardisatieorganisaties op het gebied van Post Quantum Cryptografie en Quantum Key Distribution? Wat zijn de mogelijke gevolgen wanneer andere grootmachten binnen dergelijke standaardisatieorganisaties hun invloed laten gelden en – bijvoorbeeld – QKD als primaire technologie naar voren schuiven? Wat zijn de mogelijke gevolgen voor het Nederlandse beleid? Kan de minister hier in de breedste zin op reflecteren?

Daarnaast vragen de leden van de GroenLinks-PvdA-fractie of er ook Europese standaardisatie-organisaties zijn die kaders ontwikkelen voor de transitie naar PQC en/of QKD? Kunnen deze op achterstand raken als alleen de kaders van de ISO, NIST en IETF genoemd worden in de aanbeveling? Hoe beoordeelt de minister het idee om de genoemde organisaties als een niet-uitputtende lijst op te nemen in de aanbeveling? Wat zou het nadeel zijn als uitsluitend de door het

kabinet voorgestelde standaardisatie-organisaties worden genoemd in de aanbeveling?

Ook lezen de leden van de GroenLinks-PvdA-fractie dat het kabinet van mening is dat de Routekaart naar post-quantum cryptografie aanpasbaar is, onder andere omdat de technologie nog volop in beweging is en er dus ook nog geen definitieve EU-breed gedeelde post-quantumcryptografie standaarden zijn. Deze leden prijzen de wil tot flexibiliteit van het kabinet. Tegelijk zijn zij verbaasd dat deze wil van flexibiliteit niet lijkt te gelden bij de keuze voor een specifieke technologie, gezien de voorkeur van het kabinet voor PQC ten opzichte van QKD. De leden van de GroenLinks-PvdA-fractie willen nogmaals benadrukken dat zij geen specifieke voorkeur hebben voor een van beide technologieën, maar dat zij ook graag met een open blik wensen te kijken naar beide opties. Hoe beoordeelt het kabinet de eigen wil tot flexibiliteit ten aanzien van PQC met de keuze om bij de Commissie expliciet *niet* in te zetten op QKD? Kan de minister hier in de breedste zin van het woord op reflecteren?

De leden van de GroenLinks-PvdA-fractie lezen ook dat het kabinet vindt dat de Europese routekaart uit moet gaan van een risico-gehanteerde aanpak. Wat bedoelt het kabinet hiermee? Hoe ziet het kabinet het concreet voor zich om dit voor elkaar te krijgen?

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie zien de kwantumcomputer als een veelbelovende technologie en tegelijkertijd als een groot risico voor onze (informatie)veiligheid vanwege ‘store now, decrypt later’. Deze leden hebben kennisgenomen van het Fiche aanbeveling Routekaart Post-Quantumcryptografie en hebben hierover nog enkele vragen.

Uit antwoord op schriftelijke vragen ‘Het bericht ‘NIST kiest wapens tegen kwantumcomputer als cryptokraker’ (Kamerstuk 4064) van het lid Rajkowski (VVD) blijkt dat er wordt gewerkt aan een veelzijdig programma ter bescherming van staatsgeheimen en andere informatie. Hoe verhoudt dat programma zich tot de kabinetsinzet op dit fiche, zo vragen de leden van de VVD-fractie? Ziet het kabinet Quantum Key Distribution (QKD) als een technologie waarbij het van belang om in te investeren? Zo nee, waarom niet? Zo ja op welke manier wenst zij dit vorm te gaan geven?

Gezien de snelle ontwikkelingen rondom QKD en de leidende rol van onder andere China, vragen de leden van de VVD-fractie waarom QKD niet genoemd zou kunnen worden in de aanbeveling als de EU hier samen met lidstaten wel in investeert, onder andere in het kader van de European Quantum Communication Infrastructure?

De leden van de VVD-fractie vragen welke lidstaten de visie delen van de inlichtingendiensten van Nederland, Frankrijk, Duitsland en Zweden t.a.v. het niet opnemen van QKD in de aanbeveling en in de gezamenlijke Europese routekaart. Welke doen dit niet? Wordt er samen met deze landen opgetrokken? Zo ja, hoe uit dit zich?

De leden van de VVD-fractie zijn van mening dat het belangrijk is om zich te kunnen beschermen tegen de ontwikkelingen op het gebied van QKD in grootmachten als China en de VS en hierin niet achter te lopen. Is het kabinet het hiermee eens? Wat is een mogelijk nadeel als de EU in dit stadium nog niet inzet op QKD en grootmachten als China en de VS al wel? Hoe gaat het kabinet hiermee om?

Hoe verhouden ontwikkelingen en innovaties die in Nederland plaatsvinden zich tot de Europese ambities en doelstellingen met betrekking tot post-quantumcryptografie (PQC)? De leden van de VVD-fractie vragen in hoeverre we Nederlandse ontwikkelingen kunnen versterken en beschermen met Europese doelstellingen.

Vragen en opmerkingen van de leden van de NSC-fractie

De leden van de NSC-fractie hebben kennisgenomen van het fiche over de aanbeveling Routekaart Post-Quantumcryptografie. Daarbij hebben deze leden nog enkele vragen en opmerkingen.

De leden van de NSC-fractie constateren dat het kabinet van inzicht verschilt van de Europese Commissie in enerzijds de betekenis van de term ‘hybride cryptografische constructies’ en anderzijds de beoogde rol van Quantum Key Distribution (QKD) binnen die constructies. Deze leden steunen het kabinetsstandpunt in dat het onwenselijk is om in dit stadium in te zetten op het gebruik van QKD voor beveiliging tegen de quantumdreiging en het in plaats daarvan verstandiger is om ons te richten op de migratie naar post-quantumcryptografie (PQC). Zij vragen daarbij wat het kabinet verwacht dat de potentiële toekomstige *use cases* zullen zijn voor vormen van quantumcommunicatie, waaronder QKD. Dit aangezien quantumcommunicatie als onderdeel van quantumtechnologieën in de Nationale Technologiestrategie wel wordt beschouwd als strategisch aandachtspunt. Zo heeft Nederland een trekkers- en coördinerende rol in internationale initiatieven als de Quantum Internet Alliance. Is de verwachting dat quantumcommunicatie in de toekomst wel toegevoegde waarde zal hebben voor informatiebeveiliging, of zal PQC in alle voorziene gevallen volstaan? Welke use cases buiten het domein van informatiebeveiliging voorziet het kabinet voor quantumcommunicatie en quantumnetwerken?

Het kabinet benoemt terecht het belang van inzetten op wendbaarheid van cryptografie, ook wel crypto-agility genoemd. De leden van de NSC-fractie vragen of het kabinet kan concretiseren wat de maatstaven voor crypto-agility zijn. Wanneer kan een organisatie er met een hoge mate van zekerheid op van op aan dat zij voldoende cryptografisch wendbaar is?

De leden van de NSC-fractie vragen het kabinet nader toe te lichten hoe zij de invulling van (PQC-) expertisecentra binnen Nederland voor zich ziet. Zijn deze expertisecentra specifiek bedoeld ter ondersteuning van het Rijk in de PQC-migratie of kan ook het bedrijfsleven en het maatschappelijk middenveld hiervan gebruikmaken? Indien het eerste het geval is, wat is de visie van het kabinet over hoe de in Nederland aanwezige expertise de gehele samenleving ten goede kan komen?

II Antwoord/reactie van de bewindspersoon