7-423/1

SÉNAT DE BELGIQUE

SESSION DE 2022-2023

9 FÉVRIER 2023

Proposition de résolution visant à l'instauration de mesures à l'épreuve du temps en matière d'informatique quantique

(Déposée par M. Rik Daems et consorts)

DÉVELOPPEMENTS

I. INTRODUCTION

A. Exposé du problème

Durant l'année 2023, la société IBM (*International Business Machines Corporation*) devrait lancer Condor, le premier ordinateur quantique universel au monde de plus de 1 000 qubits. IBM serait aussi sur le point de lancer Heron, le premier d'une nouvelle série de processeurs quantiques modulaires grâce auxquels elle estime pouvoir produire des ordinateurs quantiques de plus de 4 000 qubits d'ici 2025 (1). Inutile de dire que cela excède largement la puissance de calcul des ordinateurs actuels.

Bref, les ordinateurs quantiques sont des superordinateurs dont les processeurs utilisent les principes de la mécanique quantique. Cela augmente la puissance de calcul de manière exponentielle. Ces ordinateurs quantiques peuvent ainsi effectuer des calculs 10^{14} fois (soit 100 000 milliards) plus rapidement que les ordinateurs «classiques» d'aujourd'hui (2).

B. Aspects positifs des ordinateurs quantiques

Étant donné que ces ordinateurs sont capables d'effectuer des calculs beaucoup plus efficacement et donc

(1) *https://spectrum.ieee.org/ibm-condor.*
(2) *https://www.science.org/doi/10 1126/science.abe8770.*

BELGISCHE SENAAT

ZITTING 2022-2023

9 FEBRUARI 2023

Voorstel van resolutie ter invoering van toekomstbestendige maatregelen inzake *quantum computing*

(Ingediend door de heer Rik Daems c.s.)

TOELICHTING

I. INLEIDING

A. Probleemstelling

IBM's Condor, 's werelds eerste universele quantumcomputer met meer dan 1 000 qubits, zal ergens in 2023 worden gelanceerd. Ook zal IBM (*International Business Machines Corporation*) naar verwachting Heron lanceren, de eerste van een nieuwe reeks modulaire quantumprocessoren waarmee het bedrijf naar eigen zeggen tegen 2025 quantumcomputers met meer dan 4 000 qubits kan produceren (1). Nodeloos om te zeggen dat dit de rekenkracht van de huidige computers ver overstijgt.

Quantumcomputers zijn kort gezegd supercomputers waarbij de processoren gebruikmaken van de quantummechanicaprincipes. Dit verhoogt de rekenkracht exponentieel. Hiermee kunnen dergelijke quantumcomputers 10^{14} (of 100 biljoen of 100 000 miljard) keer sneller berekeningen maken dan «gewone» computers vandaag (2).

B. Positieve kanten van quantumcomputers

Doordat deze computers vele malen efficiënter berekeningen kunnen maken en dus sneller problemen

(1) *https://spectrum.ieee.org/ibm-condor.*
(2) *https://www.science.org/doi/10 1126/science.abe8770.*

de résoudre des problèmes plus rapidement que les ordinateurs actuels, la probabilité est grande que nous assistions à des avancées dans différents secteurs. Dans le domaine des sciences médicales, par exemple, des méthodes de guérison plus rapides et plus efficientes pourraient être découvertes, ce qui pourrait ouvrir la voie à un traitement et une prévention plus efficaces des maladies.

Les ordinateurs quantiques pourraient aussi être utilisés pour réaliser des innovations plus rapides en termes de produits, découvrir des moyens plus efficaces pour lutter contre le réchauffement climatique, procéder à des calculs de données plus rapides dans le monde de la finance, etc. (3).

La cryptographie quantique est utilisée aussi pour la protection des informations, plus précisément pour l'échange de clés. C'est pourquoi on l'appelle aussi la distribution quantique de clés (DQC). La DQC ne pouvant pas être craquée au moyen d'un ordinateur quantique, elle peut donc remplacer la cryptographie actuelle. Les systèmes de DQC peuvent déjà être achetés, mais ils sont encore très onéreux à l'heure actuelle.

Les systèmes de DQC utilisent une connexion directe en fibre optique ou des signaux lumineux transmis par l'air. Leur portée n'excède donc pas quelques centaines de kilomètres.

Une alternative aux systèmes de DQC est la cryptographie post-quantique. Il s'agit d'algorithmes cryptographiques qui ne peuvent pas être craqués par un ordinateur quantique. Elle peut aussi faire office de solution pour remplacer la cryptographie actuelle. On en trouve déjà des applications sur l'Internet. L'inconvénient est que cette solution est coûteuse en puissance de calcul et en bande passante.

Il faut aussi intensifier la recherche mathématique pour pouvoir apporter la preuve que cette solution est vraiment sûre. En outre, aucune norme internationale n'a encore été fixée en ce qui concerne la cryptographie post-quantique (4).

C. Aspects négatifs des ordinateurs quantiques

Pour la plupart des finalités, un ordinateur quantique n'est pas meilleur qu'un ordinateur classique. Les ordinateurs quantiques ne remplaceront donc pas totalement

(3) *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.*
(4) *https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers/informatieblad_quantumcomputers-1.pdf.*

kunnen oplossen dan de huidige computers, is de kans groot dat in we verschillende sectoren doorbraken gaan zien. Binnen de medische wetenschappen kan men, bijvoorbeeld, snellere en efficiëntere genezingsmethoden ontdekken waardoor men beter ziekten kan behandelen en voorkomen.

Quantumcomputers kunnen ook gebruikt worden om sneller productinovaties te verwezenlijken, doeltreffender manieren te ontdekken om de klimaatopwarming tegen te gaan, sneller data te berekenen in de financiële wereld, enz. (3).

Quantumcryptografie wordt ook gebruikt voor informatiebeveiliging, en specifiek voor het uitwisselen van sleutels. Het wordt daarom ook wel *quantum key distribution* (QKD) genoemd. QKD kan niet gekraakt worden met een quantumcomputer en is daarom geschikt als vervanger voor de huidige cryptografie. QKD-systemen zijn reeds te koop maar momenteel nog erg duur.

QKD-systemen maken gebruik van een directe glasvezelverbinding of van lichtsignalen die door de lucht worden verstuurd. Het bereik is daardoor niet groter dan enkele honderden kilometers.

Een alternatief voor QKD-systemen is post-quantum cryptografie. Dat zijn cryptografische algoritmes die niet gekraakt kunnen worden door een quantumcomputer. Ook deze oplossing is geschikt als vervanger voor de huidige cryptografie. Hiervan zijn al toepassingen op internet te vinden. Een nadeel is dat deze oplossing vrij veel rekenkracht en bandbreedte kost.

Er is ook meer wiskundig onderzoek nodig om er zeker van te zijn dat deze oplossing echt veilig is. Bovendien zijn er nog geen internationale standaarden afgesproken voor post-quantum cryptografie (4).

C. Negatieve kanten van quantumcomputers

Voor de meeste doeleinden is een quantumcomputer niet beter dan een gewone computer. Gewone computers zullen dus niet helemaal vervangen worden

(3) *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.*
(4) *https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers/informatieblad_quantumcomputers-1.pdf.*

les ordinateurs classiques, même si, pour certaines finalités, ils sont beaucoup plus performants que les ordinateurs classiques.

Cette technologie recèle un potentiel énorme, mais la puissance de calcul colossale qu'elle peut développer n'est pas sans risques.

Certains acteurs peuvent aussi détourner l'usage de la technologie à des fins moins positives. Cette technologie est très demandée, en particulier pour le décryptage de données confidentielles et le craquage des mesures de sécurisation actuelles, comme les mots de passe (5).

Un ordinateur quantique est très efficace pour résoudre certains problèmes mathématiques dont on a toujours pensé qu'ils étaient insolubles. Ce sont précisément les problèmes mathématiques sur lesquels notre sécurité informatique repose pour l'essentiel. Avec un ordinateur quantique, il est possible, par exemple, de décrypter le trafic internet sécurisé (*https*). Il est possible aussi de stocker le trafic internet et de le décrypter des années plus tard avec un ordinateur quantique. Cela signifie que nous devons tenir compte dès à présent de ces risques, notamment lorsqu'il s'agit d'informations qui doivent rester secrètes pendant une longue période (6).

D. Analyse de risque concernant les ordinateurs quantiques (2022)

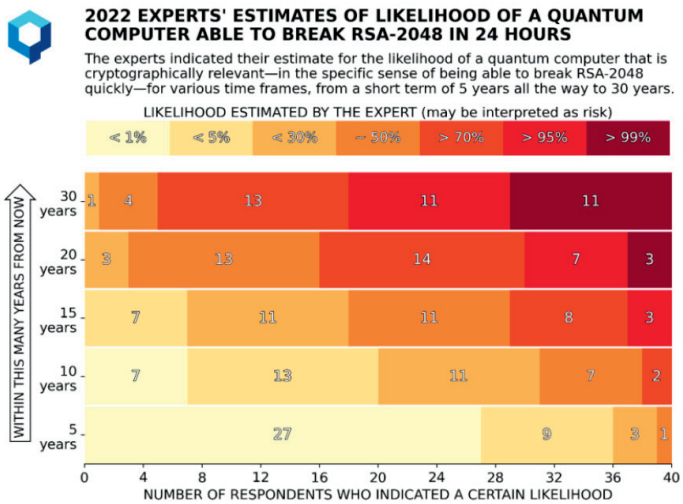
door quantumcomputers. Voor sommige doeleinden is een quantumcomputer echter veel beter dan een gewone computer.

Het potentieel van deze technologie is gigantisch maar de gigantische rekenkracht is niet zonder risico's.

Bepaalde actoren kunnen de technologie ook misbruiken voor minder positieve doeleinden. Vooral voor het ontsleutelen van vertrouwelijke data en het kraken van huidige beveiligingsmaatregelen, zoals wachtwoorden, is deze technologie gewild (5).

Een quantumcomputer is erg goed in het oplossen van bepaalde wiskundige problemen waarvan altijd gedacht werd dat ze onoplosbaar waren. Dat zijn precies de wiskundige problemen waarop een groot deel van onze informatiebeveiliging gebaseerd is. Met een quantumcomputer is het bijvoorbeeld mogelijk om beveiligd internetverkeer (*https*) te ontcijferen. Het is ook mogelijk om internetverkeer op te slaan en om het jaren later met een quantumcomputer te ontcijferen. Dat betekent dat we nu al rekening moeten houden met deze risico's, met name bij informatie die lange tijd geheim moet blijven (6).

D. Risicoanalyse omtrent quantumcomputers (2022)



Source: *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.*

Bron: *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.*

(5) *https://www.science.org/doi/10 1126/science.abe8770.*
(6) *https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers/informatieblad_quantumcomputers-1.pdf.*

(5) *https://www.science.org/doi/10 1126/science.abe8770.*
(6) *https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers/informatieblad_quantumcomputers-1.pdf.*

Il ressort de l'analyse de risque ci-dessus, réalisée par le *Global Risk Institute*, que la menace ne cesse de croître. Les avis du panel d'experts laissent entendre que la menace quantique sera inquiétante à relativement court terme, et il se pourrait bien que le danger se concrétise plus tôt que ce à quoi beaucoup s'attendent.

Assez curieusement, une majorité des répondants pensent que les investissements publics et privés globaux dans le domaine des ordinateurs quantiques continueront à croître, mais pas aussi rapidement qu'au cours des dernières années.

L'une des raisons pour lesquelles les investissements publics dans la recherche quantique ont été considérables et de longue durée réside en ce que de nombreux pays sont concernés par ce que beaucoup considèrent comme une «course internationale aux technologies quantiques». Le *Global Risk Institute* a, dans ce cadre, demandé à des experts d'indiquer quelles régions géographiques faisaient actuellement figure de précurseurs et quels pourraient être les leaders dans ce domaine dans cinq ans.

Selon les experts, l'Amérique du Nord est considérée pour l'instant comme le chef de file et elle le restera dans les cinq prochaines années, mais la Chine possède, elle aussi, un grand potentiel de croissance dans ce domaine.

La comparaison des chiffres des investissements publics mondiaux dans le domaine de l'informatique quantique donne le résultat suivant:

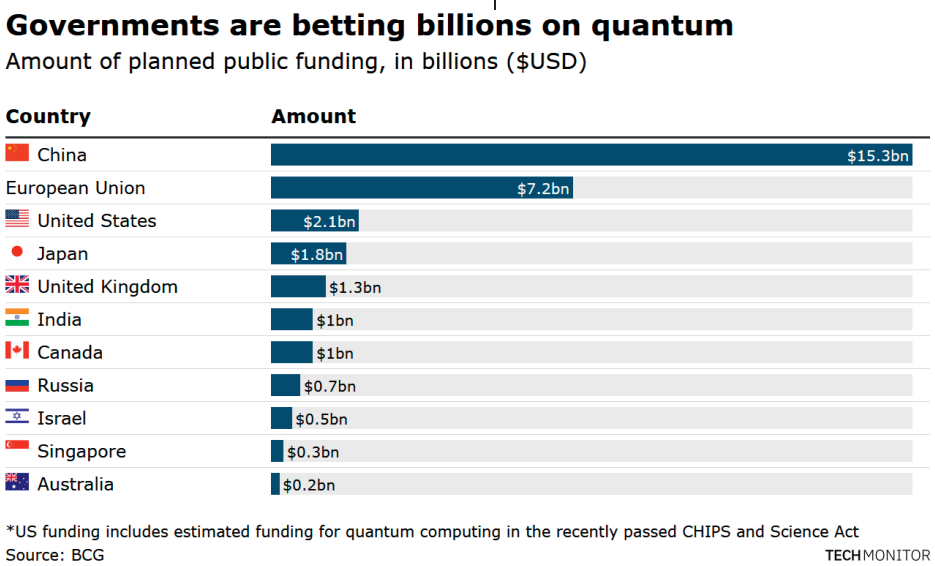
Uit de bovenstaande risicoanalyse van het *Global Risk Institute*, blijkt dat de dreiging steeds groter wordt. De adviezen van het expertenpanel suggereren dat de quantumdreiging op relatief korte termijn niet te verwaarlozen zal zijn en het zou wel eens vroeger een concreet gevaar vormen dan velen verwachten.

Het is opmerkelijk dat een meerderheid van de respondenten geloven dat de totale publieke en particuliere investeringen op het gebied van quantumcomputers zal blijven groeien, maar niet zo snel als in de afgelopen jaren.

Een van de redenen waarom de overheidsinvesteringen in quantumonderzoek groot en langdurig zijn geweest, is dat veel landen betrokken zijn bij wat door velen gezien wordt als een internationale «quantumwedloop». Het *Global Risk Institute* heeft in dit kader deskundigen gevraagd aan te geven welke geografische gebieden momenteel voorop lopen en welke de leiders kunnen zijn over vijf jaar.

Hieruit blijkt dat Noord-Amerika wordt aanzien als huidig koploper en ook nog in de komende vijf jaar, maar ook China heeft een groot groeipotentieel in dit domein.

Een vergelijking van de wereldwijde overheidsinvesteringen in quantumcomputers geeft het volgende resultaat:



Source: *https://techmonitor.ai/technology/emerging-technology/quantum-computing-germany-universal-quantum.*

Bron: *https://techmonitor.ai/technology/emerging-technology/quantum-computing-germany-universal-quantum.*

En dépit des investissements publics réalisés (voir le graphique ci-dessus), des entreprises privées américaines comme IBM et Google font actuellement la course en tête. Quant à la Chine, elle intensifie ses activités (comme le montre également le graphique). L'Union européenne (UE), en revanche, risque une fois de plus de souffrir du «paradoxe européen»: alors qu'elle dispose d'une base de recherche solide, elle reste à la traîne dès lors qu'il s'agit de transposer concrètement les idées en innovations à large spectre et, donc, de créer de la valeur. L'UE risque donc de devenir dépendante d'une tierce partie pour une autre technologie numérique fondamentale, ce qui érode encore davantage une souveraineté technologique déjà compromise dans la sphère numérique (7).

E. Accélération technologique (soudaine)

Ce domaine de recherche est le théâtre de nombreuses percées qui se succèdent à un rythme de plus en plus soutenu. Tant les avancées régulières que les progrès inattendus – ces derniers étant dès lors susceptibles de rapprocher soudainement l'échéance de la menace quantique – peuvent avoir lieu à différents niveaux de la recherche et du développement: améliorations matérielles (*hardware*), améliorations sur le plan des schémas de correction d'erreurs et améliorations dans le domaine de l'analyse cryptographique, lesquelles réduisent les moyens quantiques nécessaires pour éventuellement pirater quelques-uns des protocoles de cybersécurité les plus populaires actuellement en usage.

Avec l'arrivée imminente des ordinateurs quantiques, les acteurs malveillants n'ont pas à attendre que ce nouveau type d'ordinateurs soit disponible dans le commerce ou auprès des pouvoirs publics. Ils peuvent dès à présent intercepter, copier et sauvegarder des communications sensibles codées, en vue de les décoder ultérieurement, lorsque les ordinateurs quantiques en question seront disponibles.

Les experts en cybersécurité, eux aussi, peuvent agir dès maintenant: les récentes avancées dans le domaine des ordinateurs quantiques, ainsi que les avis formulés dans l'enquête par les experts et la forte impulsion résultant d'investissements importants consentis en la matière, doivent inciter à la prudence dans le développement de la cryptosécurité et permettre de garantir une résilience

(7) *https://il.boell.org/en/2022/01/26/german-strategy-race-quantum-computer.*

Ondanks de overheidsinvesteringen (zoals men kan zien op de bovenstaande grafiek), lopen momenteel Amerikaanse privébedrijven zoals IBM en Google voorop. China intensiveert zijn activiteiten (zie ook hierboven). De Europese Unie (EU) dreigt echter opnieuw te lijden onder de «Europese paradox»: een sterke onderzoeksbasis maar achterop hinken bij het omzetten van ideeën in breed toegepaste innovatie en dus bij het creëren van waarde. De EU dreigt dus afhankelijk te worden van een derde partij voor nog maar eens een fundamentele digitale technologie, waardoor een reeds gecompromitteerde technologische soevereiniteit in de digitale sfeer verder wordt uitgehold (7).

E. (Plotse) technologische acceleratie

Binnen dit onderzoeksveld vinden veel doorbraken plaats die elkaar steeds sneller opvolgen. Zowel gestage als onverwachte vooruitgang – waarbij de laatste mogelijk de tijdlijn van de quantumdreiging plotseling verkort – kan plaatsvinden langs verschillende lijnen van onderzoek en ontwikkeling: verbeteringen in *hardware*, verbeteringen in foutcorrectieschema's en verbeteringen in cryptoanalyse die de quantummiddelen verminderen die nodig zijn om enkele van de populairste cyberbeveiligingsprotocollen die momenteel in gebruik zijn, mogelijkerwijs te kraken.

De nakende komst van quantumcomputers maakt dat kwaadwillende actoren niet hoeven te wachten totdat deze nieuwe soort computers commercieel of van overheidswege beschikbaar zullen zijn. Zij kunnen reeds nu al gevoelige gecodeerde communicatie onderscheppen, kopiëren en opslaan, om deze op een later tijdstip, wanneer dergelijke quantumcomputers beschikbaar zijn, te decoderen.

Cyberveiligheidsspecialisten kunnen ook nu al handelen: recente vooruitgang op het gebied van quantumcomputers, samen met de adviezen van de deskundigen in de enquête en het aanzienlijke momentum dat voortkomt uit aanzienlijke investeringen op dit gebied, moeten aanzetten tot bedachtzaam handelen bij het ontwikkelen van cryptobeveiliging en voor voldoende veerkracht te

(7) *https://il.boell.org/en/2022/01/26/german-strategy-race-quantum-computer.*

suffisante face aux attaques quantiques, étant entendu qu'il faut éviter les risques supplémentaires qu'implique une transition trop hâtive (8).

II. DONNÉES ET PÉRENNITÉ TECHNOLOGIQUE (*FUTURE PROOFIN*G)

A. Introduction

Les méthodes de cryptage couramment utilisées à l'heure actuelle reposent sur l'utilisation de calculs mathématiques censés être pratiquement insolubles, du moins avec les ordinateurs actuels. L'exemple le plus célèbre est le chiffrement RSA (*Rivest, Shamir et Adlema*), basé sur la difficulté de factoriser les grands nombres, c'est-à-dire de les décomposer en facteurs premiers. De tels systèmes peuvent être craqués par des ordinateurs quantiques.

Les ordinateurs quantiques font planer une menace susceptible de provoquer une perturbation catastrophique des systèmes numériques, que ce soit par le biais d'attaques directes ou par l'érosion de la confiance dans ces systèmes informatiques (désormais totalement compromis). On peut limiter cette menace quantique en utilisant de nouveaux instruments cryptographiques résistants aux attaques quantiques. Ces instruments cryptographiques «résistants au quantique», dits aussi «post-quantiques», peuvent être conventionnels ou axés sur les technologies quantiques (9).

B. L'importance de données invulnérables aux technologies quantiques

Dès lors que la durée de confidentialité requise pour les informations sensibles est souvent longue, la menace que représentent les ordinateurs quantiques est bien réelle. Les données cryptées qui sont aujourd'hui interceptées et sauvegardées pourront être déchiffrées ultérieurement avec un ordinateur quantique, et cela pourrait se produire avant l'expiration du délai de confidentialité desdites données.

Si l'on veut migrer vers un dispositif offrant une protection contre les ordinateurs quantiques, on ne doit pas le faire trop tôt car cela risque de coûter beaucoup de temps et d'argent. Mais il ne faut pas trop tarder non plus, vu le risque auquel les données sensibles sont exposées (10).

(8) Bron: *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.*
(9) *Idem.*
(10) *https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.*

genover quantumaanvallen, waarbij de extra risico's van een overhaaste overgang moeten worden vermeden (8).

II. DATA EN *FUTURE PROOFING*

A. Inleiding

Huidige veelgebruikte encryptiemethoden vertrouwen op het gebruik van wiskundige berekeningen waarvan verwacht wordt dat ze quasi onmogelijk op te lossen zijn, althans met de huidige computers. Het bekendste voorbeeld is het *Rivest-Shamir-Adleman* (RSA) cryptobeveiligingssysteem. RSA is gebaseerd op de moeilijkheid van het vinden van priemfactoren van grote getallen. Dergelijke systemen kunnen worden gekraakt door quantumcomputers.

De dreiging die uitgaat van quantumcomputers kan leiden tot een catastrofale storing van digitale systemen, zowel door directe aanvallen als door ondermijning van het vertrouwen in deze (nu volledig gecompromitteerde) computersystemen. Een dergelijke quantumdreiging kan worden beperkt door het gebruik van nieuwe cryptografische instrumenten die bestand zijn tegen quantumaanvallen. Deze zogenaamde «*quantumsafe*» cryptografische instrumenten kunnen conventioneel of quantumgericht zijn (9).

B. Het belang van quantumveilige data

Omdat vertrouwelijke informatie vaak een lange geheimhoudingstermijn heeft, is de dreiging van een quantumcomputer reëel. Geëncrypteerde data die nu onderschept en opgeslagen worden, kunnen op een later moment ontcijferd worden met een quantumcomputer. Dat kan gebeuren voordat de geheimhoudingstermijn van deze informatie verloopt.

Te vroeg overgaan naar een quantumveilige oplossing kan veel tijd en geld kosten. Te laat is evenmin een optie omwille van het risico dat de gevoelige informatie kwetsbaar wordt (10).

(8) *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.*
(9) *Idem.*
(10) *https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.*

C. Cryptographie post-quantique (CPQ)

La cryptographie post-quantique (CPQ) est une forme de cryptographie basée sur des problèmes mathématiques qui ne peuvent pas être résolus par un ordinateur quantique. On tente actuellement d'élaborer de nouvelles normes CPQ, capables de remplacer les normes asymétriques actuelles.

Nous ne pourrons être sûrs de la fiabilité de ces nouvelles normes cryptographiques que lorsqu'elles auront eu le temps d'atteindre la maturité technologique.

La recherche scientifique contribue à accroître la confiance dans la fiabilité de ces normes. C'est un processus qui prend du temps. Aux États-Unis, l'Institut national des normes et de la technologie (*National Institute of Standards and Technology* – NIST) s'attelle déjà depuis 2016 à élaborer des normes internationales.

Ces normes sont attendues aux alentours de 2024. Le programme de recherche européen PQCRYPTO s'intéresse également aux formes de cryptographie post-quantique (11).

D. Cryptographie symétrique

La cryptographie symétrique (comme l'AES – *Advanced Encryption Standard*) permet de rendre les informations moins vulnérables aux attaques d'un ordinateur quantique. Avec un algorithme puissant comme l'AES et moyennant une longueur de clé de 256 bits, la cryptographie symétrique offre une résistance cryptographique suffisante contre les ordinateurs quantiques. Au sein d'une organisation, les longueurs de clé symétriques existantes peuvent être portées à 256 bits.

La cryptographie symétrique peut également être utilisée en complément de la protection existante. Certains produits VPN (*virtual private network*) permettent d'assurer une petite protection supplémentaire grâce à un secret partagé symétrique. On peut aussi établir des connexions (tunnels) sécurisées par une cryptographie asymétrique au moyen d'une connexion sécurisée symétrique. Les données qui seraient éventuellement interceptées resteraient ainsi protégées contre une attaque d'un ordinateur quantique. À cet égard, il est important que le mode d'échange du secret partagé symétrique résiste aux ordinateurs quantiques et que, par exemple, l'échange ait lieu hors ligne (12).

(11) *Idem*.
(12) *Idem*.

C. Post-quantum cryptografie (PQC)

Post-quantum cryptografie (PQC) is een vorm van cryptografie die gebaseerd is op wiskundige problemen die niet effectief te kraken zijn met een quantumcomputer. Op dit moment wordt gewerkt aan nieuwe PQC-standaarden, die de huidige asymmetrische standaarden kunnen vervangen.

Om zeker te zijn van de veiligheid van deze nieuwe standaarden hebben deze vormen van cryptografie tijd nodig om volwassen te worden.

Met wetenschappelijk onderzoek wordt het vertrouwen in de veiligheid van deze standaarden vergroot. Dit proces kost veel tijd. Het *National Institute of Standards and Technology* (NIST) in de Verenigde Staten is al in 2016 begonnen om internationale standaarden op punt te stellen.

Deze standaarden worden rond 2024 verwacht. Ook onderzoeksprogramma PQCRYPTO-EU doet onderzoek naar vormen van post-quantum cryptografie (11).

D. Symmetrische Cryptografie

Met symmetrische cryptografie (zoals AES – *Advanced Encryption Standard*) wordt informatie minder kwetsbaar voor aanvallen met een quantumcomputer. Met een sterk algoritme zoals AES, geeft symmetrische cryptografie met een sleutellengte van 256 bits voldoende cryptografische weerstand tegen een quantumcomputer. Binnen een organisatie kan men de bestaande symmetrische sleutellengtes verhogen naar 256 bits.

Symmetrische cryptografie kan men ook gebruiken als aanvulling op bestaande beveiliging. Met sommige VPN (*virtual private network*)-producten is het mogelijk om een extra laagje beveiliging toe te voegen met een symmetrisch gedeeld geheim. Ook kun je door asymmetrische cryptografie beveiligde verbindingen tunnelen door een symmetrisch beveiligde verbinding. Op die manier is eventueel onderschepte informatie alsnog beveiligd tegen een aanvaller met een quantumcomputer. Belangrijk hierbij is dat het gedeelde symmetrische geheim op een quantumveilige manier wordt uitgewisseld, bijvoorbeeld door het offline uit te wisselen (12).

(11) *Idem*.
(12) *Idem*.

E. Distribution quantique de clés (DQC)

La distribution quantique de clés (DQC) consiste à échanger des clés numériques au moyen de techniques issues de la mécanique quantique. Cette méthode d'échange de clés permet de détecter systématiquement toute écoute par un tiers.

Dans le cadre de la DQC, l'identité de l'émetteur et du récepteur n'est pas établie. Vous avez donc bien une connexion sécurisée, mais vous ne savez pas avec qui. Il est indispensable d'ajouter une authentification pour ne pas risquer de subir ce qu'on appelle une «attaque de l'homme du milieu». L'ajout d'une authentification est possible avec une cryptographie post-quantique ou une cryptographie symétrique et rend en fait la DQC superflue.

La DQC est réputée être une méthode d'échange de clés dont la sécurité peut être démontrée. Il n'existe actuellement encore aucune implémentation DQC ayant véritablement fait ses preuves en termes de sécurité. En l'occurrence, les preuves sont incomplètes et ne portent que sur une partie de l'application. Des hypothèses irréalistes ou irréalisables sont parfois formulées concernant le matériel (*hardware*).

Par ailleurs, la distance est limitée dans le cadre de la DQC car une liaison point à point optique est requise. Dans la pratique, on peut y remédier en utilisant des réseaux basés sur des points familiers ou on pourra, dans le futur, avoir recours à des répéteurs quantiques. En termes de coût et d'applicabilité à grande échelle, il ne s'agit pas d'alternatives intéressantes à la CPQ.

Enfin, la DQC n'offre pas une véritable alternative à la CPQ car elle s'appuie seulement sur des échanges de clés, et non sur d'autres applications telles que les signatures numériques. Le Bureau national néerlandais pour la protection des connexions (*Nationaal Bureau voor verbindingsbeveiliging* – NBV) estime qu'en raison des limitations en termes de fonctionnalités et de l'immaturité actuelle de la technologie, la DQC sans CPQ est inadéquate pour sécuriser des informations sensibles contre la menace quantique.

III. CRYPTOGRAPHIE QUANTIQUE ET MESURES

A. Mesures prises en Belgique

La note «*Stratégie cybersécurité Belgique 2.0 2021-2025*» montre que les autorités (dont le Centre pour la cybersécurité Belgique (CCB)) sont conscientes des

E. *Quantum Key Distribution* (QKD)

Quantum Key Distribution (QKD) wisselt digitale sleutels uit met technieken uit de quantummechanica. Bij deze manier van sleuteluitwisseling wordt het meeluisteren door een derde partij altijd gesignaleerd.

Met QKD wordt de identiteit van de zender en ontvanger niet vastgesteld. Je hebt dus wel een beveiligde verbinding, maar je weet niet met wie. Het toevoegen van authenticatie is een must, omdat je anders het risico loopt op een zogenaamde *man-in-the-middle*-aanval. Authenticatie toevoegen is mogelijk met PQC of symmetrische cryptografie en maakt QKD in feite overbodig.

QKD wordt genoemd als een bewijsbaar veilige methode voor sleuteluitwisselingen. Op dit moment zijn er nog geen QKD-implementaties met een passend veiligheidsbewijs. Het gaat hier bijvoorbeeld om een onvolledig bewijs door slechts een deel van de toepassing te bewijzen. Soms worden er aannames gedaan over de *hardware* die niet realistisch zijn of waar de *hardware* niet aan kan voldoen.

Daarnaast is voor QKD de afstand beperkt doordat er een optische *point-to-point*-verbinding nodig is. Dit is in de praktijk op te lossen door netwerken te gebruiken met vertrouwde punten of in de toekomst met *quantum repeaters*. Dit zijn qua kosten en schaalbaarheid geen aantrekkelijke alternatieven voor PQC.

Tot slot is QKD geen volwaardig alternatief voor PQC, omdat het zich alleen op sleuteluitwisseling richt en niet op andere toepassingen zoals digitale handtekeningen. Door de beperkingen in functionaliteit en de huidige onvolwassenheid van de technologie, is QKD zonder PQC volgens het NBV (het Nederlands Nationaal Bureau voor verbindingsbeveiliging) ongeschikt voor het beveiligen van gevoelige informatie tegen de dreiging van quantumcomputers.

III. QUANTUMENCRYPTIE EN MAATREGELEN

A. Maatregelen in België

Uit de nota «*Cybersecurity strategie België 2.0 2021-2025*», blijkt dat de autoriteiten (met name het Centrum voor cybersecurity België (CCB)) zich bewust zijn van

problèmes que poseront les ordinateurs quantiques à l'avenir.

«Il est primordial d'évaluer les risques et de mettre en place la sécurité nécessaire avant d'utiliser les nouvelles technologies. Vu la vitesse de développement et d'adoption de nouvelles technologies comme l'intelligence artificielle, le *Quantum Computing*, le *Blockchain* et les *Smart Meters&Grids*, l'enjeu réside dans l'évaluation appropriée de l'ensemble des risques (et la protection contre ces risques) (13).»

Si l'on en croit la réponse apportée une question écrite de l'auteur de la présente proposition de résolution, la Sûreté de l'État (VSSE) est bien consciente des dangers futurs que constituent les ordinateurs quantiques pour le chiffrement des données et s'intéresse à la question en permanence:

«Vu que l'on ne sait pas encore exactement quelles seront les capacités effectives des ordinateurs quantiques ni comment ceux-ci pourront être utilisés, leur impact sur le plan de la sécurité est difficile à évaluer déjà à ce stade. Il semble toutefois qu'il y ait un consensus sur le fait que les normes cryptographiques actuelles ne suffiront plus dans une ère post-quantique. La sécurité des systèmes et réseaux informatiques devra donc être revue.

La sécurité des réseaux n'est pas une mission clé de la VSSE. Le service suivra toutefois l'évolution de l'informatique quantique et évaluera quel sera l'impact de cette technologie sur les menaces dont la VSSE assure le suivi. Compte tenu de la nature de la technologie, il ne semble pas que l'informatique quantique se muera rapidement en commodité comme les smartphones, les tablettes et les ordinateurs classiques (puissants). Lorsque les ordinateurs quantiques pourront être utilisés concrètement, nous nous attendons, dans un premier temps, à une transformation dans l'espionnage d'acteurs étatiques (14).»

B. Mesures prises en Allemagne

L'Allemagne adopte une attitude proactive à l'égard des ordinateurs quantiques et des technologies qui en découlent. Cela vaut à la fois pour les investissements dans ce domaine et pour les mesures de sécurité.

(13) *https://ccb.belgium.be/sites/default/files/CCB_Strategie %20 2.0_FR_DP2.pdf.*
(14) Doc. Sénat, question écrite nº 7-1391 de Rik Daems du 27 octobre 2021 au vice-premier ministre et ministre de la Justice et de la Mer du Nord.

de problemen die quantumcomputers in de toekomst zullen doen rijzen.

«Het is van groot belang de risico's in te schatten en de nodige beveiliging op te stellen, alvorens nieuwe technologieën in gebruik te nemen. De snelheid in ontwikkeling en adoptie van nieuwe technologieën zoals Artificiële intelligentie, *Quantum Computing*, *Blockchain* en *Smart Meters & Grids* maakt een gepaste evaluatie van (en bescherming tegen) alle risico's een hele uitdaging (13).»

Uit het antwoord op een schriftelijke vraag van de indiener van dit voorstel van resolutie blijkt dat de Veiligheid van de Staat (VSSE) zich bewust is van de toekomstige gevaren van dataversleuteling en quantumcomputers en dit gestaag verder opvolgt:

«Aangezien het nog niet duidelijk is wat de effectieve capaciteiten zullen zijn van quantumcomputers en hoe die gebruikt zullen kunnen worden, is het moeilijk om nu reeds in te schatten wat de impact ervan zal zijn op de veiligheidssituatie. Er lijkt wel consensus te bestaan dat de huidige cryptografische standaarden niet meer zullen voldoen in een post-quantum tijdperk. De veiligheid van computersystemen en informaticanetwerken zal dus moeten herbekeken worden.

Netwerkveiligheid is geen kernopdracht van de VSSE. Maar de dienst zal wel de evolutie van *quantum computing* opvolgen en evalueren wat de impact van deze technologie zal zijn op de bedreigingen die de VSSE opvolgt. Gezien de aard van de technologie lijkt het niet dat *quantum computing* vlug een *commodity* zal worden zoals smartphones, tablets en klassieke (krachtige) computers. Wanneer quantumcomputers praktisch inzetbaar zullen worden, verwachten we in eerste instantie een transformatie bij *state actor* spionage (14).»

B. Maatregelen in Duitsland

Duitsland neemt een proactieve houding aan inzake quantumcomputers en daarvan afgeleide technologieën. Zowel wat betreft investeringen hierin als wat betreft veiligheidsmaatregelen.

(13) *https://ccb.belgium.be/sites/default/files/CCB_Strategie %20 2.0_NL_DP6.pdf.*
(14) Doc. Senaat, schriftelijke vraag nr. 7-1391 van Rik Daems van 27 oktober 2021 aan de vice-eersteminister en minister van Justitie en Noordzee.

Dans l'optique du BSI (*Bundesamt für Sicherheit in der Informationstechnik*), il ne s'agit plus de savoir «si» mais «quand» les ordinateurs quantiques seront disponibles. La cryptographie post-quantique deviendra la norme à terme. En fonction de l'application, il est toutefois impératif de se demander – tant à un stade précoce qu'au fur et à mesure des derniers développements – si et quand la transition vers des procédures invulnérables aux ordinateurs quantiques devra se faire.

Le premier danger des ordinateurs quantiques est qu'ils mettront en péril les systèmes fiables d'échange de clés (ils ont d'ailleurs déjà donné lieu à l'approche «stocker maintenant, décrypter plus tard» qui constitue à long terme une menace pour la sécurité).

La sécurité des clés de signature ne doit généralement être assurée qu'à court terme, mais en cas de clés de signature ayant un long délai de validité, il faudra également veiller à adopter à temps un système plus sûr. Il convient par ailleurs de tenir compte des délais de migration.

C. Mesures prises aux Pays-Bas

Le NBV (Bureau national néerlandais pour la protection des connexions) recommande l'utilisation de la CPQ (cryptographie post-quantique) (15).

Il est de plus en plus urgent de se protéger contre les ordinateurs quantiques, entre autres en ce qui concerne les informations stratégiques nécessitant un long délai de protection. C'est pourquoi le NBV néerlandais suit ces évolutions de près et impose si nécessaire des exigences complémentaires aux produits de sécurisation.

Le NBV mène aussi ses propres activités de recherche afin de développer des systèmes tels que la cryptographie post-quantique et il collabore avec d'autres organisations, comme l'Université de technologie de Delft. Il s'agit de permettre aux administrations publiques de disposer à temps de produits et solutions capables d'offrir une protection contre les ordinateurs quantiques (16).

D. Mesures prises aux États-Unis

Le président Joe Biden a déjà signé deux directives promouvant les sciences quantiques, dont un mémorandum relatif au plan gouvernemental de lutte contre les risques que représentent, pour la sécurité nationale, les

(15) *https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.*
(16) *https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers/informatieblad_quantumcomputers-1.pdf.*

Vanuit het perspectief van het BSI (*Bundesamt für Sicherheit in der Informationstechnik*) is het niet langer een kwestie van «of» maar «wanneer» er quantumcomputers komen. Post-quantum crryptografie zal op lange termijn de standaard worden. Afhankelijk van de toepassing moet echter worden overwogen – zowel in een vroeg stadium als in maat met de laatste ontwikkelingen – of en wanneer de overgang naar quantumcomputerbestendige procedures moet plaatsvinden.

In eerste instantie zullen quantumcomputers vooral een gevaar vormen voor veilige sleuteluitwisselingssystemen (en dus al aanleiding hebben gegeven tot het concept «nu opslaan, later ontsleutelen» als bedreiging voor de veiligheid op lange termijn).

Ondertekeningssleutels hoeven meestal alleen op korte termijn veilig te zijn, maar in het geval van ondertekeningssleutels met een lange geldigheidsduur zal ook een tijdige overgang noodzakelijk zijn. Er moet ook rekening worden gehouden met migratietermijnen.

C. Maatregelen in Nederland

Het NBV (Het Nederlands Nationaal Bureau voor verbindingsbeveiliging) adviseert het gebruik van PQC (post-quantum cryptografie) (15).

De weerbaarheid tegen quantumcomputers wordt steeds urgenter, met name voor strategische informatie met een lange beschermingstermijn. Daarom volgt het NBV deze ontwikkelingen op de voet en stelt waar nodig aanvullende eisen aan beveiligingsproducten.

Het NBV doet ook eigen onderzoek naar ontwikkelingen als post-quantum cryptografie en werkt samen met andere organisaties zoals de Technische Universiteit Delft. Inzet is het tijdig beschikbaar krijgen van producten en oplossingen binnen de overheid, die beveiliging kunnen bieden tegen quantumcomputers (16).

D. Maatregelen in de Verenigde Staten

President Joe Biden heeft reeds twee richtlijnen ter bevordering van de quantumwetenschappen ondertekend, waaronder ook een memorandum rond het plan van zijn regering om nationale veiligheidsrisico's aan te pakken

(15) *https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.*
(16) *https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers/informatieblad_quantumcomputers-1.pdf.*

ordinateurs quantiques capables de craquer le chiffrement opéré par le ministère de la Défense (17).

S'il se réjouit des nombreuses applications prometteuses de l'informatique quantique (*quantum information science* – QIS), le gouvernement Biden reconnaît aussi que les progrès des technologies quantiques constituent un risque spécifique pour la sécurité économique et nationale de l'Amérique.

La *Defense Information Systems Agency* (DISA) collabore avec le *National Institute of Standards and Technology* et le DoD (*Department of Defense*) pour développer des algorithmes invulnérables aux ordinateurs quantiques, a déclaré dernièrement l'*Emerging Technologies Directorate's chief engineer* de la DISA (18).

IV. QUE PROPOSONS-NOUS?

Nous pensons qu'il est impératif que les autorités scrutent en détail notre économie nationale, notre sécurité et nos secteurs sensibles et identifient les risques potentiels liés à l'avènement des ordinateurs quantiques.

Dans les entreprises comme dans les organismes publics, on ne saurait trop insister sur l'importance de répertorier les mesures cryptographiques actuelles, de déterminer si ces mesures sont ou non pérennes et d'en connaître les implications.

À cet égard, il est capital d'investir à la fois dans le développement de ces technologies et dans les analyses d'impact qui s'y rapportent, en particulier pour accélérer la migration vers des mesures de sécurité améliorées.

La présente proposition de résolution a un caractère transversal. Les TIC (technologies de l'information et de la communication), la politique scientifique, la vie privée et la sécurité sont des matières transversales.

*
* *

(17) *https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.*
(18) *https://breakingdefense.com/2022/05/new-white-house-directive-warns-of-cryptological-risks-from-quantum-computers/.*

veroorzaakt door quantumcomputers die de encryptie van het ministerie van Defensie kunnen kraken (17).

Hoewel de regering Biden «de vele veelbelovende toepassingen van QIS (*quantum information science*)» verwelkomt, erkent zij ook dat de vooruitgang in quantumtechnologieën een specifiek risico vormt voor de economische en nationale veiligheid van Amerika.

Het *Defense Information Systems Agency* (DISA) werkt samen met het *National Institute of Standards and Technology* en het DoD (*Department of Defense*) om quantum-bestendige algoritmen te ontwikkelen voor militair gebruik, verklaarde *DISA's Emerging Technologies Directorate's chief engineer* onlangs (18).

IV. WAT STELLEN WIJ VOOR?

Voor ons is het van groot belang dat de overheid onze nationale economie, veiligheid en gevoelige sectoren screent op mogelijke risico's in het licht van de komst van quantumcomputers.

Zowel bij bedrijven als overheidsorganisaties kan niet genoeg het belang benadrukt worden van het in kaart brengen van de huidige cryptografische maatregelen, of deze maatregelen al dan niet toekomstbestendig zijn en wat de implicaties hiervan zijn.

Investeren in zowel de ontwikkeling van dergelijke technologie als impact-analyses hierrond, in het bijzonder om de migratie naar geüpgradede veiligheidsmaatregelen te bespoedigen, zijn hierbij van groot belang.

Dit voorstel van resolutie heeft een transversaal karakter. ICT (*information and communication technology*), wetenschapsbeleid, privacy en veiligheid zijn transversale aangelegenheden.

*
* *

(17) *https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.*
(18) *https://breakingdefense.com/2022/05/new-white-house-directive-warns-of-cryptological-risks-from-quantum-computers/.*

PROPOSITION DE RÉSOLUTION

Le Sénat,

A. considérant que les ordinateurs quantiques ont une vitesse de calcul 100 000 milliards de fois supérieure à celles des ordinateurs «classiques»;

B. considérant que la probabilité est grande que les ordinateurs quantiques réalisent des percées importantes dans plusieurs secteurs, ce qui pourrait bouleverser en premier lieu le paysage technologique, médical et socio-économique;

C. considérant que la technologie quantique peut non seulement décrypter l'information, mais aussi la sécuriser;

D. considérant que la technologie quantique peut être détournée pour voler des données confidentielles et percer les mesures de sécurité actuelles;

E. considérant qu'une analyse de risque réalisée par le *Global Risk Institute* montre que la probabilité que les ordinateurs quantiques déchiffrent les méthodes de cryptage actuelles ne cesse d'augmenter;

F. considérant que l'Amérique du Nord est considérée comme le *leader* actuel en technologie quantique et maintiendra son avance pendant les cinq prochaines années, mais que la Chine dispose également d'un potentiel de croissance important dans ce domaine;

G. considérant que l'Union européenne (UE) risque de souffrir à nouveau du «paradoxe européen», qui est de disposer d'une base de recherche solide, mais de trop tarder à convertir les idées en innovations à large spectre et donc à créer de la valeur;

H. considérant que des acteurs malveillants sont d'ores et déjà en mesure d'intercepter, de copier et de stocker des communications confidentielles cryptées pour les décoder ultérieurement, lorsque ces ordinateurs quantiques seront disponibles;

I. considérant que les ordinateurs quantiques pourront craquer les cryptages de sécurité que nous utilisons couramment, comme le chiffrement RSA (*Rivest-Shamir-Adleman*);

J. considérant que la cryptographie post-quantique (CPQ) est basée sur des problèmes mathématiques qu'un ordinateur quantique ne pourra craquer efficacement;

VOORSTEL VAN RESOLUTIE

De Senaat,

A. overwegende dat quantumcomputers 100 000 miljard keer sneller berekeningen kunnen maken dan «gewone» computers;

B. overwegende dat dankzij quantumcomputers de kans groot is dat we in verschillende sectoren diverse doorbraken gaan zien, die in eerste instantie het technologische, medische en socio-economische landschap kunnen doorheen schudden;

C. overwegende dat quantumtechnologie niet alleen informatie kan kraken maar ook kan beveiligen;

D. overwegende dat quantumtechnologie misbruikt kan worden om vertrouwelijke data te stelen en huidige beveiligingsmaatregelen te kraken;

E. overwegende dat uit een risicoanalyse van het *Global Risk Institute* blijkt dat het risico dat de huidige versleutelingsmethoden gekraakt worden door deze technologie steeds groter wordt;

F. overwegende dat Noord-Amerika wordt aanzien als huidig koploper inzake quantumtechnologie en ook nog in de komende vijf jaar, maar ook China heeft een groot groeipotentieel binnen dit domein;

G. overwegende dat de Europese Unie (EU) opnieuw dreigt te lijden onder de «Europese paradox»: met name een sterke onderzoeksbasis, maar achterophinken bij het omzetten van ideeën in breed toegepaste innovatie en dus bij het creëren van waarde;

H. overwegende dat kwaadwillende actoren nu al gevoelige gecodeerde communicatie kunnen onderscheppen, kopiëren en opslaan, om deze op een later tijdstip, wanneer dergelijke quantumcomputers beschikbaar zijn, te decoderen;

I. overwegende dat huidige veelgebruikte veiligheidsencrypties zoals RSA (*Rivest-Shamir-Adleman*) kunnen worden gekraakt door quantumcomputers;

J. overwegende dat post-quantum cryptografie (PQC) gebaseerd is op wiskundige problemen die niet effectief te kraken zijn met een quantumcomputer;

K. considérant que la cryptographie symétrique (comme l'AES – *Advanced Encryption Standard*) rend les informations moins vulnérables aux attaques des ordinateurs quantiques;

L. considérant que la distribution quantique de clés (DQC) consiste à échanger des clés numériques en recourant à des techniques issues de la mécanique quantique, ce qui signifie que l'écoute non sollicitée effectuée par des tiers sera toujours détectée;

M. considérant que des instances belges spécialisées, telles que la Sûreté de l'État (VSSE) et le Centre pour la cybersécurité Belgique (CCB), identifient et surveillent en permanence les risques posés par les ordinateurs quantiques;

N. considérant que l'Allemagne adopte une attitude proactive à l'égard des ordinateurs quantiques et des technologies qui en découlent et que cela vaut à la fois pour les investissements et pour les mesures de sécurité;

O. considérant que les Pays-Bas estiment qu'il est de plus en plus urgent de se protéger contre les ordinateurs quantiques, entre autres en ce qui concerne les informations stratégiques nécessitant un long délai de protection;

P. considérant que les États-Unis reconnaissent tant les potentialités que les risques technologiques des ordinateurs quantiques et qu'ils sont déjà en train d'élaborer des stratégies à cet égard;

Q. considérant que si l'on veut migrer vers un dispositif offrant une protection contre les ordinateurs quantiques, on ne doit pas le faire trop tôt car cela risque de coûter beaucoup de temps et d'argent, mais que l'on ne doit pas trop tarder non plus, au vu du risque auquel les données sensibles sont exposées,

Demande à tous les gouvernements compétents en la matière:

1) de faire en sorte que les instances compétentes lancent un processus de screening numérique de notre économie nationale, de notre sécurité et de nos secteurs sensibles et identifient les risques auxquels ceux-ci sont potentiellement exposés en raison de l'avènement des ordinateurs quantiques;

2) d'être attentifs aux risques que les banques de données des pouvoirs publics subissent des intrusions commises

K. overwegende dat symmetrische cryptografie (zoals AES – *Advanced Encryption Standard*) ervoor zorgt dat informatie minder kwetsbaar wordt voor aanvallen met een quantumcomputer;

L. overwegende dat *Quantum Key Distribution* (QKD) digitale sleutels uitwisselt met technieken uit de quantummechanica, waardoor het ongevraagd meeluisteren door een derde partij altijd gesignaleerd wordt;

M. overwegende dat gespecialiseerde instanties in België, zoals de Veiligheid van de Staat (VSSE) en het Centrum voor cybersecurity België (CCB), de risico's van quantumcomputers erkennen en blijvend opvolgen;

N. overwegende dat Duitsland een proactieve houding aanneemt inzake quantumcomputers en daarvan afgeleide technologieën, zowel wat betreft investeringen als wat betreft veiligheidsmaatregelen;

O. overwegende dat Nederland de weerbaarheid tegen quantumcomputers als steeds urgenter beschouwt, met name voor strategische informatie met een lange beschermingstermijn;

P. overwegende dat de Verenigde Staten zowel de technologische mogelijkheden als risico's omtrent quantumcomputers erkennen en reeds strategieën hierrond aan het uitwerken zijn;

Q. overwegende dat te vroeg overgaan naar een quantumveilige oplossing veel tijd en geld kan kosten, maar te laat overschakelen evenmin een optie is, door het risico dat gevoelige informatie kwetsbaar wordt,

Vraagt aan alle hiertoe bevoegde regeringen om:

1) de bevoegde instanties een digitaal screeningsproces te laten starten omtrent onze nationale economie, onze veiligheid en onze gevoelige sectoren en daaraan de mogelijke risico's te koppelen bij de komst van quantumcomputers;

2) aandacht te hebben voor mogelijke intrusies in overheidsdatabanken door kwaadwillende actoren met

par des acteurs malveillants à l'aide d'ordinateurs quantiques et de prendre aussi, éventuellement, des mesures supplémentaires;

3) de mener une étude dans laquelle les modèles de menace en matière de technologie quantique et les solutions y afférentes sont couplés à une perspective tant régionale et nationale qu'internationale;

4) d'amplifier les connaissances existantes en ce qui concerne le cryptage et la sécurité des données, sur la base d'approches pluridisciplinaires et de solutions multiples, en s'appuyant sur l'expertise existante en matière de cybersécurité, de technologies de l'information et de la communication d'enseignement et de sécurité;

5) de maintenir un contact permanent avec des acteurs tels que les services de sécurité, les experts en sécurité informatique, les universités et les entreprises afin d'avoir une meilleure connaissance des risques inhérents à la technologie quantique et de parvenir à des solutions qualitatives;

6) d'examiner dans quelle mesure la Belgique peut jouer un rôle de pionnier en Europe dans le développement et l'utilisation de cette nouvelle technologie, en étant surtout attentifs à l'applicabilité pratique de la technologie quantique;

7) d'examiner dans quelle mesure la Belgique peut jouer un rôle de pionnier en matière de recherche scientifique (comme c'est le cas pour le projet PQCRYPTO EU) sur la standardisation des méthodes de cryptage post-quantique;

8) d'examiner dans quelle mesure nos différentes autorités peuvent lancer d'ores et déjà des campagnes d'information ou de sensibilisation à l'intention aussi bien des entreprises et des secteurs sensibles que du grand public, en ce qui concerne le cryptage supplémentaire des banques de données sensibles existantes et la nécessité de rendre celui-ci durable dans une ère post-quantique;

9) d'examiner quelles méthodes de cryptage (comme la CPQ, la cryptographie symétrique, la DQC, etc.) sont les plus adaptées et pour quels secteurs, en tenant compte

behulp van quantumcomputers en eventueel ook extra maatregelen te nemen;

3) een onderzoek te openen waarbij men dreigingsmodellen omtrent quantumtechnologie en daarbij horende oplossingen koppelt aan zowel een regionaal, nationaal als internationaal perspectief;

4) voort te bouwen op bestaande kennis op het gebied van encryptie en dataveiligheid, vanuit multidisciplinaire benaderingen en meervoudige oplossingen, voortbouwend op de bestaande deskundigheid inzake cyberveiligheid, informatie- en communicatietechnologie onderwijs en beveiliging;

5) in voortdurend contact te staan met actoren zoals de veiligheidsdiensten, beveiligingsexperts, universiteiten en de bedrijfswereld om een beter zicht te krijgen op de risico's van quantumtechnologie, en te komen tot kwaliteitsvolle oplossingen;

6) na te gaan in hoeverre België binnen Europa een voortrekkersrol kan opnemen bij het ontwikkelen en gebruiken van deze nieuwe technologie, met daarbij een focus op praktische toepasbaarheid van quantumtechnologie;

7) te onderzoeken in hoeverre België een voorttrekkersrol kan opnemen inzake wetenschappelijk onderzoek (zoals met PQCRYPTO-EU) over de standaardisering van post-quantum encryptiemethoden;

8) na te gaan in hoeverre onze diverse overheden reeds informatie- of bewustwordingscampagnes kunnen starten voor zowel bedrijven, gevoelige sectoren als het brede publiek over extra versleuteling van bestaande gevoelige databanken en het «*futur proof*» maken van dergelijke versleutelingen in een post-quantum tijdperk;

9) te onderzoeken welke versleutelingsmethoden (zoals PQC, symmetrische cryptografie, QKD, enz.) het best aansluiten bij welke sectoren, rekening houdend

de facteurs tels que les coûts, la sensibilité des données et la faisabilité, et de formuler des recommandations à cet effet.

Le 19 janvier 2023.

met factoren zoals kosten, gevoeligheid van de data en haalbaarheid en hiervoor aanbevelingen uit te werken.

19 januari 2023.

Rik DAEMS.
Nadia EL YOUSFI.
Gaëtan VAN GOIDSENHOVEN.
Ludwig VANDENHOVE.
Philippe DODRIMONT.

Imprimerie centrale – Centrale drukkerij