2
Vragenuur

Aan de orde is **het mondelinge vragenuur**, overeenkomstig artikel 136 van het Reglement van Orde.

Vragen van het lid Elissen aan de minister van Veiligheid en Justitie over **ingebouwde "achterdeurtjes" in computerchips uit China**.

De **voorzitter**:
Ik heet de minister van Veiligheid en Justitie van harte welkom. U bent populair vanmiddag. Er zullen immers twee vragen aan u worden gesteld.

☐

De heer **Elissen** (PVV):
Voorzitter. Recent werd bekend dat bepaalde Chinese microchips een achterdeur bevatten. Via deze achterdeur kunnen kwaadwillenden de chips op afstand herprogrammeren, zodat zij computersystemen kunnen afluisteren, overnemen of uitschakelen. Ik vraag de minister van Veiligheid en Justitie wat hierop de reactie van de Nederlandse overheid is. Klopt het dat inlichtingendiensten hiervoor al lang geleden waarschuwden? Zo ja, wat is er gedaan met die waarschuwingen? Welke stappen gaat de minister van Veiligheid en Justitie zetten, met welke andere bewindspersonen gaat hij die afstemmen en hoe ziet hij de respons van de Nederlandse overheid voor zich? Is inmiddels reeds bekend of chips met achterdeurtjes in Nederland in gebruik zijn, bijvoorbeeld in openbaarvervoerssystemen, bij banken of bij onze strijdkrachten? Zitten er überhaupt Chinese chips in het materieel van onze strijdkrachten verwerkt? Kan voorkomen worden dat chips met achterdeurtjes in ons materieel terechtkomen?

Ongeveer twee maanden geleden verschenen er berichten uit Australië dat bij het aanbesteden van de ruggengraat van het Australische internet bedrijven uit China werden uitgesloten. Zal de Nederlandse overheid bij het aanbesteden van cruciale systemen leveranciers uit landen als China voortaan niet meer laten meedingen? Wat zijn hiervoor de mogelijkheden? Kunnen we Chinezen die een achterdeur komen aanbieden, de draaideur wijzen? Hebben we hierbij, net zoals bij het drugsdebat, weer een probleem met de achterdeur?

De **voorzitter**:
Minister Opstelten, u hebt twee minuten spreektijd voor het antwoord.

☐

Minister **Opstelten**:
Voorzitter. Fijn dat u dat nog een keer zegt. De tijd gaat nu in. Ik dank de heer Elissen voor zijn vraag. Het onderzoek is aangekondigd met een persbericht. Op 9 tot 12 september vindt de presentatie van het onderzoek tijdens een workshop in Leuven plaats. De inlichtingendiensten zijn bekend met het probleem. Wij zullen het op de voet volgen. De heer Elissen vroeg welke stappen wij zullen zetten. Zoals hij ongetwijfeld weet, hebben de minister van Binnenlandse Zaken, ikzelf en VNO-NCW het rapport Kwetsbaarheidanalyse Spionage Nederland uitgebracht. In dat rapport staan alle stappen beschreven.

Ook vroeg de heer Elissen of deze achterdeurtjes in de chips bekend zijn. Dit probleem is bekend. Vandaar hebben wij die kwetsbaarheidsanalyse opgesteld. Wij volgen het op de voet. Het rapport gaat echter niet alleen daarover.

Kan de invoer ervan worden voorkomen? Ik kan daarvoor geen garanties geven, maar wij zullen dit natuurlijk ten volle proberen te voorkomen met het Nationaal Cyber Security Centrum. Wij bedienen ons hierbij ook van de AIVD en het Nationaal Bureau voor Verbindingsbeveiliging. Daarnaast zullen wij natuurlijk met onze internationale contacten in de onderzoekswereld en in de wereld van de veiligheidsdiensten maatregelen nemen, als die moeten worden genomen. Ook zullen wij ervoor zorgen dat dit niet kan gebeuren.

De heer **Elissen** (PVV):
Voorzitter. Ik begrijp dat de inlichtingendiensten hiervan op de hoogte waren. Dat is prima. Ik begrijp ook dat er nu een onderzoek is aangekondigd. Ik ben zeer benieuwd naar de uitkomsten van dat onderzoek. Wij zullen die zeker gaan volgen in Leuven op 9 tot 12 september. De vraag blijft of wij voldoende waren toegerust en waren voorbereid op de Chinese achterdeurchips.

Over het Nationaal Cyber Security Centrum en de Nationale Cyber Security Strategie is nog weleens onduidelijkheid geweest. Mijn vraag is met name wie hierover de leiding heeft. Is dat inderdaad de minister van Veiligheid en Justitie vanuit het perspectief dat deze vinding een risico voor de nationale veiligheid heeft blootgelegd of wellicht omdat er sprake kan zijn van spionage? Is er in de Nationale Cyber Security Strategie dus voorzien in een dergelijk scenario? Vindt de minister dat we hier te maken hebben met de voorbereidingshandelingen van cyberwarfare? Is het in dat geval slechts een taak van Defensie? Zo ja, heeft Defensie voldoende onderzoekscapaciteit? Heeft Defensie voldoende capaciteit om Nederland te beschermen? Of is het dan toch een taak voor Veiligheid en Justitie in verband met staatsveiligheid en vanuit de regie- en coördinatiefunctie, die wat ons betreft duidelijk bij de minister van Veiligheid en Justitie thuishoort?

Minister **Opstelten**:
Zijn wij voldoende voorbereid? Over die vraag hebben we in debatten al vele malen gesproken. Daarom is de Kwetsbaarheidsanalyse Spionage er niet voor niets. Gelet op de vragen, is dit voor mij de kans om iedereen te vragen om scherp te blijven. Zowel de overheid als het bedrijfsleven doen dit. Dat is heel belangrijk. Wij laten daar onderzoek naar doen door de Inspectie Veiligheid en Justitie. Het Nationaal Cyber Security Centrum (NCSC) heeft daarin de leiding. Ik ben verantwoordelijk voor de coördinatie van de cyber security. Daar is mijn collega van Binnenlandse Zaken bij betrokken inzake de overheid, evenals mijn collega's van Defensie, van Buitenlandse Zaken en van EL&I. Ik wil die taken niet overnemen.

Is hier sprake van cyberwarfare? Wij hebben nu niet de feiten. Op basis van deze berichten is er naar onze mening geen aanleiding om ons zorgen te maken. We zullen dit wel keihard met alle diensten op de voet volgen.

De heer **Elissen** (PVV):
Stel dat we op basis van de feiten wel tot de conclusie zouden komen dat er sprake kan zijn van cyberwarfare.

Zou in dat geval de minister van Veiligheid en Justitie dan ook regie blijven voeren, coördinatie houden en zich laten bijstaan door de vakminister van Defensie?

Minister **Opstelten**:
In een kabinet laat een minister zich nooit bijstaan door een collega. Dat is natuurlijk collegiaal. Ik treed niet in de plaats van de minister van Defensie. Die is daar ten volle voor verantwoordelijk. Ik voer wel de regie en zorg ervoor dat wij dat met elkaar doen en dat er één strategie is vanuit alle ministers inzake ons land en samen met het bedrijfsleven, de particuliere markt.

De **voorzitter**:
Tot slot, mijnheer Elissen.

De heer **Elissen** (PVV):
Tot slot. Ook ik probeer scherp te blijven, maar ik heb nog geen antwoord gehad op de vraag over de aanbesteding. Is de minister net als Australië bereid om risicolanden zoals China uit te sluiten?

Minister **Opstelten**:
Op dit moment is daartoe geen aanleiding. Als de gegevens daar wel aanleiding toe zouden geven, schromen wij natuurlijk niet om de maatregelen te nemen die nodig zijn. Dan zal ik de Kamer laten weten welke maatregelen dat zijn.

De heer **El Fassed** (GroenLinks):
De minister zegt dat hij geen aanleiding ziet om ons zorgen te maken. Tegelijkertijd vraag ik mij wel af of er bij de rijksoverheid, bij Defensie en EL&I, voldoende kennis in huis is om ervoor te zorgen dat we ons inderdaad geen zorgen hoeven te maken. Worden er voldoende hardwaretesten uitgevoerd om dit soort specifieke problemen te constateren?

Minister **Opstelten**:
Deze vraag is zeer relevant. We zijn continu bezig om onze kennis te verhogen en te vermeerderen. Daarom is het Nationaal Cyber Security Centrum er ook. We doen dat ook bij onze nationale veiligheidsdiensten. De KWAS, de Kwetsbaarheidsanalyse Spionage, die ik net heb genoemd, wil ik toch nog een keer in herinnering brengen. Die brengt ook met zich mee dat niet alleen de overheid maar ook het bedrijfsleven zich ten volle bewust moet zijn van de risico's hier.

Mevrouw **Gesthuizen** (SP):
Ik wil iets meer boter bij de vis. Ik wil graag dat deze minister hier een en ander toezegt. Dat kan hij samen met de minister van Binnenlandse Zaken en het liefste ook met de minister van Defensie. Hij moet de Kamer van dit proces op de hoogte gaan houden, want ik ben allerminst gerustgesteld. Als dit, zoals de minister zegt, nu wordt uitgezocht, wil ik graag dat de Kamer hiervan op de hoogte wordt gesteld, als het kan voor het zomerreces, in ieder geval zodra het mogelijk is.

Minister **Opstelten**:
Tegenover mevrouw Gesthuizen herhaal ik wat ik zojuist heb gezegd over de KWAS. Het gaat hier over de kwetsbaarheid voor spionage, waarover mijn collega van Binnenlandse Zaken en ik en VNO-NCW die kwetsbaarheidsanalyse hebben uitgebracht. Wij proberen het bedrijfsleven te stimuleren en om zelf taken uit te oefenen. De inspectie van Veiligheid en Justitie onderzoekt onafhankelijk hoe wij dat doen. Ik zal de Kamer in de loop van het jaar informeren over de stand van zaken.

De heer **Schouw** (D66):
Ik weet niet of de minister ons geruststelt. Ik vind dat het erger wordt. Waar rook is, is vuur. Is de minister bereid om desnoods vertrouwelijk de Kamer binnen een maand te informeren over wat er aan de hand is? Ik kan namelijk geen chocola maken van het antwoord dat de minister hier geeft.

Minister **Opstelten**:
Ik dacht dat ik op de vraag van de heer Elissen bijzonder helder had geantwoord. Ik kan het nog een keer herhalen. Over de persberichten, niet meer dan dat. Er zal een presentatie plaatsvinden van het onderzoek, dat wij nog niet kennen, in Leuven van begin september. Wij zullen daarbij zijn en dat op de voet volgen, maar niet dankzij het persbericht. Wij waren het al van plan. Ik zal de Kamer gewoon informeren over wat daar is gepresenteerd, de consequenties en hoe wij erin zitten. Dat is geen enkel punt.

De **voorzitter**:
Dank u wel. Wij zijn nu toe aan de tweede serie vragen.