Ministerie van Defensie

Ministerie van Defensie

Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Plein 2
2511 CR Den Haag

Onze referentie
2018024323

Bij beantwoording datum, onze referentie en betreft vermelden.

Datum 4 oktober 2018
Betreft Verstoring Russische cyberoperatie in Den Haag

In deze brief informeer ik u, mede namens de minister van Buitenlandse Zaken en de minister van Justitie en Veiligheid, over een cyberoperatie van de Russische militaire inlichtingendienst GRU in Den Haag, waarover ik met de directeur van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de ambassadeur van het Verenigd Koninkrijk vandaag een persconferentie heb gegeven. Aanvankelijk zou vanuit het Verenigd Koninkrijk de *Minister of State for Europe and the Americas* de persconferentie met mij geven, maar door een geannuleerde vlucht is dat helaas niet mogelijk gebleken.

De MIVD heeft met ondersteuning van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en een Britse partnerdienst op vrijdag 13 april jl. een cyberoperatie van de GRU in Den Haag verstoord. Deze operatie was gericht tegen de internationale Organisatie voor het Verbod op Chemische Wapens (OPCW). Russische inlichtingenofficieren waren in de nabijheid van het hoofdkwartier van de OPCW in Den Haag voorbereidingen aan het treffen om de netwerken van de OPCW te hacken. Zij waren in het bezit van specialistische apparatuur waarmee Wifi-verkeer kon worden onderschept of worden gemanipuleerd. Nederland heeft als gastland een speciale verantwoordelijkheid voor internationale organisaties om hen vrij en veilig hun werk te kunnen laten doen. Om de integriteit van deze internationale organisatie te beschermen, is de cyberoperatie van de GRU vroegtijdig door de MIVD verstoord en zijn de Russische inlichtingenofficieren dezelfde dag het land uit begeleid. De MIVD doet onderzoek naar de apparatuur van de inlichtingenofficieren die is achtergebleven in Nederland.

Uit onderzoek naar de apparatuur is gebleken dat deze ook actief is geweest in Brazilië, Zwitserland en Maleisië. Zoals ook in de persconferentie van de Britse *Minister of State* aan de orde kwam, was één van de in Nederland actieve Russische inlichtingenofficieren ook actief in de GRU-operatie gericht op het MH17-onderzoek in Maleisië. De Tweede Kamer is eerder geïnformeerd dat er dossiers en (politieke) processen zijn die voor Rusland van belang zijn en waar manipulatie en beïnvloeding een voorstelbare dreiging zijn, zoals het MH17-dossier (kamerstuk 26643, nr. 496). De organisaties die betrokken zijn bij het strafrechtelijk onderzoek en de aansprakelijkstelling van de Russische Federatie zijn zich bewust van digitale dreigingen en hebben gepaste maatregelen getroffen. Samen met partners gaat het OM in het *Joint Investigation Team* door met het strafrechtelijke onderzoek naar het neerhalen van MH17.

Het is niet gebruikelijk om met concrete resultaten van inlichtingendiensten naar buiten te treden. Het kabinet kiest er nu echter bewust voor deze operatie en daarmee de betrokken Russische inlichtingenofficieren publiek te maken, zodat hen het internationaal opereren moeilijker wordt gemaakt. Het ondermijnen van de integriteit van internationale organisaties is onaanvaardbaar. Nederland heeft als gastland een speciale verantwoordelijkheid voor internationale organisaties om hen vrij en veilig hun werk te kunnen laten doen. Dit is ook de boodschap die vandaag wordt overgedragen aan de tijdelijke zaakgelastigde van de Russische Federatie, die op het ministerie van Buitenlandse Zaken is ontboden. Nederland zal in internationaal verband, zoals binnen de EU en de NAVO, het ondermijnende gedrag van de Russische militaire inlichtingendienst aan de orde stellen.

Nederland deelt de zorgen van internationale partners met betrekking tot het schadelijke en ondermijnende gedrag van de GRU in het digitale domein. Nederland ondersteunt dan ook de conclusie van het Verenigd Koninkrijk zoals vandaag gepresenteerd: de GRU ondermijnt de internationale rechtsorde met dergelijke cyberoperaties. Dit past in het dreigingsbeeld zoals uiteengezet in de jaarverslagen van MIVD en AIVD en het Cyber Security Beeld Nederland, en in het patroon zoals geschetst in eerdere verklaringen van het Verenigd Koninkrijk. Statelijke actoren richten zich steeds meer op digitale spionage en vormen de grootste dreiging voor de digitale veiligheid van Nederland.

Vandaag treedt de VS naar buiten met een aanklacht tegen diverse Russische inlichtingenofficieren. Op 6 augustus jl. heeft het Amerikaanse *Department of Justice* in het kader van een strafrechtelijk onderzoek naar ongeoorloofde Russische cyberoperaties een rechtshulpverzoek bij het Nederlandse Openbaar Ministerie ingediend. Het OM heeft ter uitvoering van dit rechtshulpverzoek informatie aan de VS verstrekt gebaseerd op een ambtsbericht van de MIVD. Daarnaast is het OM een eigen onderzoek gestart.

Met het openbaar maken van deze operatie wil het kabinet duidelijk maken dat actoren achter dergelijke cyberaanvallen niet langer ongestoord kunnen opereren. Zoals uiteengezet in de Nederlandse Cyber Security Agenda en de Geïntegreerde Buitenland- en Veiligheidsstrategie, vraagt de cyberdreiging om heldere nationale en internationale respons. Het kabinet heeft in het kader van de nationale veiligheid structureel extra middelen ter beschikking gesteld aan onder andere het Nationaal Cyber Security Centrum en de inlichtingen- en veiligheidsdiensten. Nederland investeert in het bestendigen van internationale afspraken gebaseerd op het internationaal recht en in cybercapaciteiten ter respons op en ter afschrikking van cyberaanvallen. Dat is nodig om cyberdreigingen vroegtijdig te kunnen detecteren, resoluut af te weren en proportioneel op te kunnen treden.

DE MINISTER VAN DEFENSIE

Drs. A.Th.B. Bijleveld-Schouten