Ministerie van Defensie

> Retouradres Postbus 20701 2500 ES Den Haag

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

Ministerie van Defensie

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

Onze referentie
BS2017031604

Datum
Betreft Antwoorden op de vragen over het bericht dat geprobeerd wordt de smartphones van NAVO-troepen te hacken.

Bij beantwoording datum, onze referentie en betreft vermelden.

Hierbij ontvangt u de antwoorden op de schriftelijke vragen van het lid Popken (PVV) over het bericht dat geprobeerd wordt de smartphones van NAVO-troepen te hacken (ingezonden op 6 oktober 2017 met kenmerk 2017Z13380).

DE MINISTER VAN DEFENSIE

Mr. dr. K.H.D.M. Dijkhoff

Antwoorden op de schriftelijke vragen van het lid Popken (PVV) over het bericht dat geprobeerd wordt de smartphones van NAVO-troepen te hacken (ingezonden op 6 oktober 2017 met kenmerk 2017Z13380).

1
Bent u bekend het bericht 'Russia has been hacking smartphones of NATO troops'? 1)

Ja.

2
Kunt u aangeven of er ook bij de Nederlandse militairen meldingen van (vermoedens van) hacken zijn binnengekomen tijdens de militaire oefening in de Baltische landen?

4
Kunt u aangeven of er in het verleden vaker tijdens NAVO-oefeningen meldingen van cyber-dreigingen zijn binnengekomen?

Antwoord op de vragen 2 en 4:

Om redenen van operationele veiligheid kan ik hierover geen uitspraken doen.

3
Kunt u aangeven welke maatregelen het Nederlandse leger neemt tegen het hacken van smartphones van defensie medewerkers?

Defensie moet zijn voorbereid op cyberdreigingen en zich hiertegen kunnen beschermen om de inzetbaarheid van de krijgsmacht te garanderen. De verdediging tegen digitale aanvallen is in de Defensie Cyber Strategie dan ook als speerpunt bestempeld (33 321 nr. 1, 27 juni 2012). Netwerken en systemen zijn kwetsbaar voor aanvallen en verstoringen. De verdediging hiertegen behelst onder andere het monitoren en het analyseren van dataverkeer, het onderkennen van digitale aanvallen en de reactie hierop. Defensie moet daartoe bekend zijn met de mogelijke dreigingen in het digitale domein en de kwetsbaarheden van haar eigen netwerken en systemen. Vanuit veiligheidsoverwegingen kan ik hierop niet verder ingaan.

5
Bent u bereid dit onderwerp binnen de NAVO bespreekbaar te maken zodat gezamenlijk tot oplossingen gekomen kan worden? Zo nee, waarom niet?

Mede door Nederlandse initiatieven heeft *cyber defence* reeds de structurele aandacht van het bondgenootschap. Zoals het kabinet heeft aangegeven bij de beantwoording van de vragen van de Tweede Kamer over de Internationale cyberstrategie (26 643 nr. 475, 1 juni 2017), zijn de NAVO-lidstaten het erover eens dat het bondgenootschap sterker staat wanneer de lidstaten hun cyber security op orde hebben. Daarom is door alle lidstaten met de *Cyber Defence Pledge* de belofte uitgesproken dat de inspanningen op het gebied van cyber security blijvend worden verhoogd. Binnen de NAVO is het *NATO Communications and Information Agency* (NCIA), waarvan de *NATO Computer Incident Response Capability* een onderdeel is, verantwoordelijk voor de bescherming van de eigen

IT-netwerken en IT-systemen van de Navo tijdens missies en operaties. Tot slot vormen cyber security aspecten een steeds belangrijker onderdeel bij NAVO-oefeningen, trainingen en opleidingen.

1) http://nypost.com/2017/10/04/russia-has-been-hacking-smartphones-of-nato-troops/