Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Vragen gesteld door de leden der Kamer

2023Z06033

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Russische hackers trainen voor aanvallen op kritieke infrastructuur»* (ingezonden 5 april 2023).

Vraag 1
Bent u bekend met het bericht dat Russische hackers trainen voor aanvallen op kritieke infrastructuur?[1]

Vraag 2
Bent u op de hoogte van softwareprogramma's en projecten, zoals Scan-V en Crystal-2V, die als doel hebben om cyberaanvallen (op kritieke infrastructuur) te stimuleren? Herkent het u dit verontrustende beeld van Russische cyberoperaties, gericht op onze vitale infrastructuur, zoals spoorwegen, vliegvelden, en elektriciteitsnetwerken? Zo ja, hoe beoordeelt u dit beeld?

Vraag 3
Hoe staat het met de versterkte aanpak vitaal? Acht u de toegezegde stappen en acties afdoende in het kader van de Russische voornemens om cyberaanvallen op onze kritieke infrastructuur uit te voeren? Zo ja, kunt u dit toelichten? Zo nee, welke aanvullende acties acht u noodzakelijk?

Vraag 4
Welke maatregelen neemt u om onze vitale infrastructuur beter te beschermen tegen digitale aanvallen via de toeleveringsketen ook wel «supply chain» cyberaanvallen genoemd?

Vraag 5
Kunt u een update geven over de voortgang en de uitkomsten van het overheidsbreed cyberprogramma? In hoeverre is Nederland voorbereid op eventuele cyberaanvallen?

[1] NRC, 31 maart 2023, «Russische hackers trainen voor aanvallen op kritieke infrastructuur» (https://www.nrc.nl/nieuws/2023/03/31/russische-hackers-trainen-voor-aanvallen-op-kritieke-infrastructuur-a4160986).

Vraag 6
Hoe frequent wordt er binnen de vitale sectoren geoefend met het anticiperen op digitale aanvallen op onze vitale infrastructuur? Wordt hierbij ook geoefend op scenario's van uitval van kritieke diensten? Zo nee, waarom niet?

Vraag 7
Wanneer was de laatste digitale oefening op cyberaanvallen en welke lessen zijn hieruit getrokken? Wat zijn de vervolgstappen om beter voorbereid te zijn op eventuele cyberaanvallen?

Vraag 8
Bent u het met de stelling eens dat het belangrijk is om regelmatig te oefenen met het bestrijden van cyberaanvallen zodat Nederland voorbereid is op actuele dreigingen? Zo ja, wanneer is de eerstvolgende cross-sectorale cyberoefening? Welke oefeningen staan gepland op de langere termijn? Hoe staat het met structureel organiseren van cross-sectorale cyberoefeningen? Zo nee, waarom niet?