Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2389

Vragen van het lid **Dijkhoff** (VVD) aan de ministers van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht dat de Verenigde Staten al langer zuchten onder cyberaanvallen* (ingezonden 11 april 2013).

Antwoord van minister **Opstelten** (Veiligheid en Justitie), mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 27 mei 2013). Zie Aanhangsel Handelingen, vergaderjaar 2012–2013, nr. 2188.

Vraag 1
Bent u bekend met het bericht «VS zuchten al langer onder cyberaanvallen»?[1]

Antwoord 1
Ja.

Vraag 2, 3 en 5
Is het waar dat een radicale hackactivistengroep genaamd «Cyber Fighters of Izz ad-Din al-Qassam» verantwoordelijk is voor cyberaanvallen op financiële instellingen in de VS?
Welke informatie is bekend over deze groepering? Staat deze groepering op een terreurlijst, bijvoorbeeld de terreurlijst van de EU?
Kunt u aangeven of deze groepering feitelijk door een staat wordt aangestuurd, in die zin dat de staat verantwoordelijk is voor de cyberaanvallen? Zo ja, om welke staat gaat het?

Antwoorden 2, 3 en 5
Een groep die zichzelf Cyber Fighters of Izz ad-Din al-Qassam noemt, heeft de verantwoordelijkheid voor meerdere grootschalige aanvallen op de financiële sector in de Verenigde Staten opgeëist. Deze groepering staat niet op de EU- of een nationale terrorismelijst. In de media is gesuggereerd dat de Iraanse overheid een relatie heeft met de Cyber Fighters of Izz ad-Din al-Qassam. De Iraanse overheid heeft publiekelijk ontkend betrokken te zijn bij de cyberaanvallen op de Amerikaanse banken. Bij het Nationaal Cyber Security Centrum en de inlichtingen- en veiligheidsdiensten is bekend dat statelijke actoren of aan staten gelieerde actoren zich in toenemende mate in het digitale domein

[1] http://www.telegraaf.nl/digitaal/21461949/__VS_zuchten_al_langer_onder_cyberaanvallen__.html.

ah-tk-20122013-2389
ISSN 0921 - 7398
's-Gravenhage 2013

begeven. De AIVD onderzoekt de herkomst van dergelijke cyberaanvallen, maar kan in het openbaar geen mededelingen doen over de uitkomst van deze onderzoeken.

Vraag 4
Worden de banktegoeden van deze groepering of daaraan gelieerde personen bevroren? Zo nee, bent u bereid u (al dan niet in internationaal verband) ervoor in te zetten dat dit zal gaan gebeuren?

Antwoord 4
Aangezien de groepering niet op een sanctielijst voorkomt, zijn eventuele tegoeden niet bevroren. Nederland beschikt niet over informatie die als basis zou kunnen voor een voorstel tot het bevriezen van tegoeden. Ik zie voor nu dan ook geen aanknopingspunten om hier in internationaal verband voor te pleiten.

Vraag 6
Door wie of wat wordt deze groepering gefinancierd? Kunnen deze financiers strafrechtelijk worden vervolgd?

Antwoord 6
Informatie over de financieringsbronnen van de groep die de verantwoordelijkheid heeft opgeëist is niet beschikbaar. Generiek kan ik aangeven dat het financieren van cybercriminaliteit in de vorm van een DDos-aanval in Nederland, in voorkomende gevallen, strafbaar is als deelneming aan het misdrijf belemmeren van de toegang of het gebruik van geautomatiseerde werken (artikel 138b Sr).

Vraag 7 en 8
Zijn de recente DDos-aanvallen op Nederlandse financiële instellingen ook afkomstig van deze groepering? Zo nee, kunt u aangeven welke groepering dan wel verantwoordelijk is voor deze aanvallen en of dit eveneens een groepering is met een ideologische inslag?
Wat is de omvang van de schade van deze cyberaanvallen op Nederlandse banken? Vinden deze aanvallen plaats om financiële fraude te verhullen of wordt hiermee een ideologisch doel gediend?

Antwoorden 7 en 8
Op dit moment voert het Team High Tech Crime van de politie op last van het Openbaar Ministerie een onderzoek uit naar de DDos-aanvallen. Dit onderzoek is in volle gang, daarmee is het onmogelijk om nu al uitspraken te doen over mogelijke daders en/of motieven. Er zijn vooralsnog geen aanwijzingen dat de genoemde groepering verantwoordelijk is voor de cyberaanvallen op de Nederlandse banken. Bij DDos-aanvallen is de website van een bank tijdelijk onbereikbaar doordat grote hoeveelheden verkeer worden verstuurd naar de website. Daardoor is het uitvoeren van transacties onmogelijk. Er is echter nadrukkelijk geen sprake van het ontvreemden van tegoeden van klanten. Daardoor wordt dus geen schade geleden. Wel is het mogelijk dat klanten tijdelijk geen transactie hebben kunnen uitvoeren. De schade van het niet op dat moment uit kunnen voeren van transacties valt moeilijk in te schatten.

Vraag 9
Is er al contact geweest met de VS over de cyberaanvallen? Zo nee, waarom niet? Zo ja, welke afspraken zijn er gemaakt?

Antwoord 9
Ondermeer het NCSC en de AIVD hebben regelmatig contact met enerzijds het onder het Department of Homeland Security ressorterende US-Cert (Computer Emergency Response Team), en anderzijds de Amerikaanse Inlichtingen en Veiligheidsdiensten. In deze contacten wisselen het centrum en de diensten onder meer kennis en informatie uit. Ook gerubriceerde informatie over digitale aanvallen kan daarbij worden gedeeld. Over internationale samenwerking met deze diensten in concrete gevallen doen wij in het openbaar geen uitspraken.

Vraag 10
Is de Algemene Inlichtingen en Veiligheidsdienst (AIVD) in voldoende mate toegerust om met betrekking tot deze nieuwe vormen van terrorisme de veiligheid van Nederland te waarborgen en inlichtingen daaromtrent te vergaren?

Antwoord 10
Contraterrorisme en cyber security zijn, zowel afzonderlijk als in samenhang, prioriteiten van de AIVD. Om de technologische ontwikkelingen op dit gebied bij te houden zal daarin de komende jaren verder geïnvesteerd moeten worden.

Vraag 11
Welke concrete acties gaat u naar aanleiding van deze aanvallen nemen dan wel heeft u reeds genomen?

Antwoord 11
In onze brief d.d. 16 april heb ik samen met de Minister van Financiën de Tweede Kamer ingelicht over de ondernomen acties. In het kader van de actieve informatie-uitwisseling met de banken is het belangrijk dat met hen is afgesproken dat een liaison in het NCSC wordt geplaatst om de intensieve samenwerking te bestendigen. Daarnaast heb ik de Kamer geïnformeerd over het nog dit jaar actualiseren van de Nationale Cyber Security Strategie met als belangrijk onderdeel het samen met de AIVD en de MIVD op- en uitbouwen van een Nationaal Detectie en Response Netwerk. Daarnaast zal de aanpak van «Botnets» (netwerken van geïnfecteerde computers die gebruikt kunnen worden bij een (DDos) aanval) worden geïntensiveerd en zal het juridisch instrumentarium worden aangepast aan de ontwikkelingen in het digitale domein.