// Tweede Kamer der Staten-Generaal **2**

Vergaderjaar 2018–2019 **Aanhangsel van de Handelingen**

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

1853

Vragen van het lid **Van Dam** (CDA) aan de Minister van Justitie en Veiligheid over *het bericht «Cyberaanval kopen lijkt kattenkwaad, maar is een misdaad»* (ingezonden 6 februari 2019).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 14 maart 2019) Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 1727.

Vraag 1
Kent u het artikel «Cyberaanval kopen lijkt kattenkwaad, maar is een misdaad»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u aangeven in hoeverre u bekend bent met de geschetste problematiek omtrent platformcriminaliteit waar illegale diensten (zoals malware, exploit-kits en DDoS-aanvallen) worden aangeboden? Is het strafbaar om deze diensten aan te bieden dan wel om deze te gebruiken? Welke activiteiten ondernemen politie, justitie, het Nationaal Cyber Security Centrum (NCSC) en andere (overheids)diensten om te voorkomen dat deze diensten worden aangeboden dan wel om op te treden tegen dit soort aanbieders?

Vraag 5
Kunt u aangeven in hoeverre het een obstakel vormt voor de opsporing dat aanbieders van dergelijke platformen anoniem op het darkweb opereren?

Antwoord 2 en 5
Het is bekend dat technisch vaardige cybercriminelen hun criminele diensten en/of software waarmee criminaliteit kan worden gepleegd, op internet aanbieden. Dit fenomeen wordt aangeduid als cybercrime-as-a-service («CaaS») en wordt onder meer genoemd in het Cyber Security Beeld Nederland 2018. Het aanbieden en het gebruiken van dergelijke diensten of technische hulpmiddelen, of enkel het vervaardigen, verwerven of voorhanden hebben van bepaalde software is onder voorwaarden (bijvoorbeeld dat

[1] AD/Haagsche Courant, 31 januari 2019

ah-tk-20182019-1853
ISSN 0921 - 7398
's-Gravenhage 2019

de software in objectieve termen is aan te merken als geschikt tot plegen van een misdrijf in de zin van artikel 138ab, eerste lid, 138b of 139c of artikel 138ab, tweede of derde lid) strafbaar indien het oogmerk van het plegen van strafbare feiten aanwezig is (art. 139d, tweede en derde lid Sr). Naast het vervaardigen, voorhanden hebben of aanbieden van dergelijke middelen zijn de feiten die daarmee vervolgens worden gepleegd ook strafbaar.[2] De aanbieders van de middelen zijn vervolgens (als medeplegers/ medeplichtigen) tevens strafbaar voor die feiten, naast de gebruikers van hun diensten.

De politie en het Openbaar Ministerie voeren opsporingsonderzoeken uit naar aanbieders en gebruikers van strafbare diensten of hulpmiddelen. Een betrouwbare inschatting van het aantal aanbieders en gebruikers in Nederland is niet goed mogelijk, mede gelet op de eenvoud waarmee dergelijke diensten mondiaal kunnen worden geproduceerd en aangeboden. Strafrechtelijk optreden is mogelijk door opsporing en vervolging, en door het ontoegankelijk maken van online marktplaatsen, websites of delen daarvan. Een veel voorkomende complicatie voor de politie en het Openbaar Ministerie is dat dergelijke websites en aanbieders door anonimiseringstechnieken, het routeren van internetverkeer door meerdere landen of het gebruikmaken van virtuele servers, vaak zeer lastig of helemaal niet zijn op te sporen. Desalniettemin boeken de politie en het Openbaar Ministerie successen, veelal met internationale partners en Europol.
Het aantal opsporingsonderzoeken naar cybercrime is de afgelopen jaren gestaag gegroeid. De aanpak van cybercrime is ook in de nieuwe Veiligheidsagenda een prioriteit. Met de additionele middelen die in het Regeerakkoord zijn vrijgemaakt voor de politie en de strafrechtketen wordt de komende jaren onder meer geïnvesteerd in kennis en capaciteit bij de politie en het Openbaar Ministerie voor de aanpak van cybercrime. Het Nationaal Cyber Security Centrum (NCSC) levert als informatieknooppunt en expertisecentrum voor cybersecurity ondersteuning en advies aan Rijkoverheids- en vitale organisaties. Het NCSC werkt samen met overheden, bedrijven en de wetenschap om kennis over DDoS-aanvallen en de bescherming daartegen uit te wisselen.[3]

Vraag 3
Welk beeld heeft u van de laagdrempeligheid en toegankelijkheid van dergelijke diensten die worden aangeboden door cybercriminelen aan de gewone burger? Bestaan er in de regelgeving voldoende barrières om het gebruik van deze illegale diensten tegen te gaan?

Antwoord 3
De regering staat voor een open, vrij en veilig internet. Dat biedt vele economische en maatschappelijke kansen en mogelijkheden. Tegelijk kunnen criminelen die openheid en vrijheid ook misbruiken, bijvoorbeeld door het aanbieden van criminele diensten, anoniem en vanaf een onbekende plek in de wereld. Door de hoogwaardige Nederlandse digitale infrastructuur en snelle internetverbindingen is het zeer aannemelijk dat infrastructuur waarmee criminele activiteiten worden gepleegd, zich ook in ons land bevindt. Zelfreguleringsinitiatieven leveren een belangrijke bijdrage om crimineel gebruik van de Nederlandse infrastructuur zo veel mogelijk te voorkomen.[4]
Cybercrime-as-a-service maakt technisch complexe criminele handelingen voor minder technisch onderlegde daders gemakkelijk bereikbaar, terwijl de opsporing zeer lastig is.

Vraag 4
Welke mogelijkheden biedt de wet Computercriminaliteit III om platformcriminaliteit tegen te gaan en de aanbieders van dergelijke platformen(strafrechtelijk) aan te pakken?

---

[2] Zie ook de eerste richtlijn voor strafvordering cybercrime van het Openbaar Ministerie van 1 februari 2018: https://www.om.nl/@101753/richtlijn-8/

[3] https://www.ncsc.nl/actueel/factsheets/factsheet-technische-maatregelen-voor-de-continuiteit-van-onlinediensten.html

[4] https://ecp.nl/activiteiten/abusebestrijding-2–0/

Antwoord 4
De wet Computercriminaliteit III bevat een bevoegdheid voor de politie tot het heimelijk en op afstand binnendringen in geautomatiseerd werk. Vervolgens kunnen aan dat geautomatiseerde werk of aan de daarin opgeslagen digitale gegevens onderzoekshandelingen worden verricht. Het ontoegankelijk maken van gegevens is daarbij een mogelijkheid waarin de wet voorziet. Die bevoegdheid kan worden ingezet voor de opsporing van strafbare feiten met een strafbedreiging van 8 jaar of meer en strafbare feiten die in het Besluit Onderzoek in Geautomatiseerd Werk[5] zijn aangewezen. Cybercrime-as-a-service betreft veelal strafbare feiten die in het Besluit zijn aangewezen, zoals bijvoorbeeld computervredebreuk (art. 138ab Sr), al dan niet gericht tegen de vitale infrastructuur, DDoS-aanvallen (art. 138b Sr) en het opzettelijke vernielen van een geautomatiseerd werk (art. 161sexies Sr). Daarnaast bevat de wet een verheldering van de bevoegdheid tot het vorderen van het ontoegankelijk maken van gegevens (art. 125p Sv). Deze bevoegdheid kan onder meer worden toegepast voor het ontoegankelijk maken van een website die illegale diensten of technische hulpmiddelen aanbiedt.

Vraag 6
Klopt het dat gebruikers van dergelijke platformen eenvoudiger op te sporen zijn dan de aanbieders? Biedt het wetboek of de richtlijnen van het Openbaar Ministerie mogelijkheden om aanbieders strenger te straffen dan gebruikers van deze platformen?

Antwoord vraag 6

Het gebruik van digitale anonimiseringstechnieken of versleutelde communicatiediensten is voor individuele gebruikers net zo eenvoudig als voor de aanbieders van CaaS-platformen. De vaardigheden van de gebruikers of aanbieders, ook wel de «human factor», is vaak van doorslaggevend belang bij een succesvolle opsporing en vervolging.
De «richtlijn voor strafvordering cybercrime»[6] van het Openbaar Ministerie geeft aanknopingspunten voor een hogere strafreis bij verdachten die meermalen strafbare feiten hebben gepleegd, veelal in georganiseerd verband en in combinatie met andere strafbare feiten. Bij aanbieders zal doorgaans vaker van (één van) deze strafverzwarende factoren sprake zijn dan bij gebruikers. Daarbij wordt ook een onderscheid gemaakt tussen *first offenders* en gevallen van recidive. Een onderscheid tussen aanbieders en gebruikers als zodanig maakt de richtlijn echter niet.
De praktijk van verhuur van «virtuele serverruimte» zorgt ervoor dat de eigenaar van een datacentrum vaak niet weet welke klanten welk deel van de servercapaciteit huurt, waardoor het opsporen van aanbieders (van bijvoorbeeld CaaS-platformen) zeer lastig is. De eigenaar van een datacentrum of de *reseller* van servercapaciteit daarbinnen hebben beiden geen verplichting om een klantenregister bij te houden.

[5] Stb. 2018, nr. 340
[6] Stcr. 2018, nr. 3271.