Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
3896100

Uw kenmerk
2022Z03923

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 21 april 2022
Onderwerp Antwoorden Kamervragen over het bericht 'Ddos'er die fiscus, banken en Tweakers aanviel, krijgt 200 uur taakstraf'

In antwoord op uw brief van 1 maart 2022 deel ik u mee, mede namens de minister voor Rechtsbescherming, dat de schriftelijke vragen van de leden Ellian en Rajkowski (beiden VVD) inzake het bericht 'Ddos'er die fiscus, banken en Tweakers aanviel, krijgt 200 uur taakstraf' worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Minister van Justitie en Veiligheid,

D. Yeşilgöz-Zegerius

Antwoorden van de ministers van Justitie en Veiligheid en voor Rechtsbescherming op schriftelijke vragen van de leden Rajkowski en Ellian (beiden VVD) over het bericht 'DDoS'er die fiscus, banken en Tweakers aanviel, krijgt 200 uur taakstraf'
(Ingezonden 1 maart 2022, 2022Z03923)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Datum
21 april 2022

Ons kenmerk
3896100

Vraag 1
Bent u bekend met het bericht 'DDoS'er die fiscus, banken en Tweakers aanviel, krijgt 200 uur taakstraf'[1]?

Antwoord op vraag 1
Ja.

Vraag 2
Worden DDoS-aanvallen die zijn uitgevoerd op vitale diensten door het openbaar ministerie (OM) bij het bepalen van de strafeis en bij de rechter bij de strafoplegging als een strafverzwarende omstandigheid gezien?

Antwoord op vraag 2
Ja. Het OM houdt bij het bepalen van de strafeis rekening met de wettelijke strafmaxima zoals geformuleerd in het Wetboek van Strafrecht (Sr). Uit artikel 138b lid 3 Sr volgt dat het strafmaximum van twee naar maximaal vijf jaar gevangenisstraf kan gaan indien een DDoS-aanval is gepleegd tegen een geautomatiseerd werk behorende tot de vitale infrastructuur[1].

Vraag 3
Hoeveel veroordelingen zijn bekend van zaken waarbij een DDoS-aanval gepleegd is?

Antwoord op vraag 3
Bij een DDoS-aanval kan artikel 138b Sr (opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren door daaraan gegevens aan te bieden of toe te zenden) of artikel 161sexies Sr (misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht) tenlastegelegd worden. In de periode 2019 – 2021 zijn er 8 veroordelingen geweest voor artikel 138b. Onder de delictsomschrijving van artikel 161sexies vallen echter meer delicten dan alleen een DDoS-aanval. Er kan in de informatiesystemen van de Rechtspraak niet worden achterhaald hoeveel veroordelingen op basis van artikel 161sexies een DDoS-aanval betroffen. Het totale aantal veroordelingen van artikel 161sexies geeft daarom geen representatief beeld van het aantal veroordelingen van DDoS-aanvallen.

[1] Onder vitale infrastructuur wordt verstaan: 'een voorziening, systeem of deel daarvan op het grondgebied van een lidstaat, dat van essentieel belang is voor bijvoorbeeld het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, zoals energiecentrales, vervoersnetwerken, of overheidsnetwerken, en waarvan de verstoring of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ongeregeld zouden raken' (Kamerstukken II 2014/15, 34034, 3, p. 9).

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Datum
21 april 2022

Ons kenmerk
3896100

Vraag 4
Deelt u de mening dat deze vormen van cybercriminaliteit hard aangepakt moeten worden vanwege de grote maatschappelijke impact?

Antwoord op vraag 4
Zeker. Cybercrime kan een grote impact hebben op individuele slachtoffers en de maatschappij als geheel. Gedurende de coronacrisis zijn we in het dagelijks leven steeds afhankelijker geworden van de online wereld. Dit maakt dat cyberaanvallen een groot risico vormen voor onze maatschappij. Het Cybersecurity Beeld Nederland benoemt ransomware zelfs als een risico voor onze nationale veiligheid.[2] Adequate opsporing en vervolging van daders is noodzakelijk. Het internet mag geen vrijplaats zijn voor criminelen. Opsporing, vervolging en verstoring is één van de vier sporen van de integrale aanpak van cybercrime. Hierover wordt uw Kamer jaarlijks geïnformeerd per brief.[3]

Vraag 5
Hoe vaak vindt er recidive plaats bij de cybercriminelen die DDoS-aanvallen hebben gepleegd? Wordt er onderzoek gedaan naar het recidiverisico bij cyberdelicten?

Antwoord op vraag 5
Hierover zijn geen cijfers beschikbaar. Voor zover bekend lopen er momenteel geen onderzoeken naar het recidiverisico bij cyberdelicten. Wel is door het WODC onderzoek gedaan naar cyberdaders, waarover uw Kamer is geïnformeerd.[4] Dit onderzoek gaf aan dat voor daders van cybercrime geen eenduidig profiel bestaat, maar dat er kenmerken zijn die relatief vaker voorkomen bij cyberdaders dan bij traditionele daders of vrij uniek zijn voor cyberdaders. Zo plegen jongere daders strafbare feiten in eerste instantie vaker uit nieuwsgierigheid, intellectuele uitdaging of leergierigheid, en zijn zich niet altijd bewust van de strafbaarheid. Ook bleek uit het onderzoek dat bij het voorkomen van recidive klassieke interventies bruikbaar zouden kunnen zijn, indien ze zouden worden aangepast aan de digitale context. Zie hiervoor vraag 6.

Vraag 6
Welke maatregelen en middelen worden ingezet om recidive bij cyberdelicten te voorkomen?

Antwoord op vraag 6
Bij de aanpak van cybercrime wordt een onderscheid gemaakt tussen cybercrimedelicten in enge zin (zoals ransomware- en DDoS-aanvallen) en gedigitaliseerde delicten (zoals online fraude). Onderzoek geeft aan dat er kenmerken zijn die relatief vaker voorkomen bij cyberdaders dan bij traditionele daders of vrij uniek zijn voor cyberdaders.[5] Ten behoeve van deze specifieke doelgroep maken Halt, de Raad voor de Kinderbescherming (RvdK) en de Reclassering gebruikt van de Hack_Right-aanpak. Daarnaast is de bestaande leerstraf Tools4U van de RvdK aangevuld voor daders van gedigitaliseerde delicten.

---

[2] Cybersecuritybeeld Nederland 2021 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)
[3] Kamerstukken II, 2020/21, 26 643, nr. 768
[4] Kamerstukken II, 2019/20, 26 643, nr. 696
[5] Cyberdaders: uniek profiel, unieke aanpak? (wodc.nl)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Datum
21 april 2022

Ons kenmerk
3896100

Ook is het instrumentarium voor risicotaxatie aangepast. Voor jeugdige justitiabelen is het landelijk risicotaxatie-instrumentarium (LIJ) aangevuld zodat het nu ook kan worden gebruikt in het geval zij een cybercrime of gedigitaliseerd delict hebben gepleegd. Dit jaar wordt gemonitord of de huidige aanpassingen voldoen of dat nog verdere aanvullingen nodig zijn.

Vraag 7
Hoe vaak wordt bij strafoplegging of bij een OM-afdoening de aanvullende interventie Hack_Right toegepast? Wat zijn hier tot nu toe de resultaten van en kunt u deze resultaten met de Kamer delen?

Antwoord op vraag 7
Sinds 2019 zijn er 25 zaken afgerond. Hack_Right kan worden ingezet in het kader van een Halt-afdoening, een (jeugd)reclasseringsbegeleiding, als taakstraf of als gedragsaanwijzing in het kader van een bijzondere voorwaarde (volwassenenreclassering). De afgelopen jaren is de interventie Hack_Right (door)ontwikkeld en is toegewerkt naar indiening van de interventie bij de Erkenningscommissie Justitiële Interventies van het Nederlands Jeugdinstituut (NJi). Medio 2022 wordt de interventie voor erkenning voorgelegd.

Vraag 8
Welke criteria worden gehanteerd om te bepalen of Hack_Right kan worden toegepast?

Antwoord op vraag 8
Hack_Right is bedoeld voor jongeren en jongvolwassenen die minimaal 12 en maximaal 24 jaar oud zijn ten tijde van het plegen van het delict, (gedeeltelijk) bekennen een cyberdelict[6] te hebben gepleegd, niet eerder veroordeeld zijn voor een cyberdelict, affiniteit hebben met ICT en gemotiveerd zijn om deel te nemen aan Hack_Right. In uitzonderingsgevallen kan een lange variant van Hack_Right – op verzoek van een rechter, officier van justitie of een van de ketenpartners – ook ingezet worden voor jongvolwassenen van 24 tot 30 jaar. Bij deze doelgroep is het extra belangrijk dat bij de invulling van Hack_Right wordt aangesloten bij ontwikkelingstaken van jongvolwassenen op het gebied van werk, opleiding, vrijetijdsbesteding en relaties.

De langere variant van Hack_Right kan bij Reclassering worden opgelegd in het kader van een bijzondere voorwaarde, en bij de RvdK in het kader van een werkstraf. Hack_Right kan ook worden opgelegd in de vorm van een Halt-afdoening. Dit betreft een kortere variant.

Vraag 9
Deelt u de mening dat de interventie Hack_Right een positieve bijdrage kan leveren aan het voorkomen van recidive bij jonge cybercriminelen? Zo ja, welke stappen onderneemt u om dit nadrukkelijker in het beleid naar voren te laten komen? Zo nee, waarom niet?

Antwoord op vraag 9
Minderjarigen kunnen, soms onbewust, forse cyberdelicten plegen. Hack_Right heeft als doel recidive onder jonge cybercriminelen te voorkomen en tegelijkertijd hun maatschappelijk zeer relevante ICT-talent te stimuleren binnen de kaders van de wet. Doordat jongeren leren hoe zij deze talenten op een veilige en rechtmatige manier kunnen ontwikkelen en inzetten, kan toekomstige

[6] Cybercrimedelicten zijn delicten waarbij ICT zowel het doel als het middel is.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Datum
21 april 2022

Ons kenmerk
3896100

maatschappelijke en financiële schade voorkomen worden. In de uitvoering van de interventie worden (private) ICT-bedrijven en –afdelingen betrokken, om de jongere te begeleiden bij de ontwikkeling van diens talent voor legale doeleinden. Momenteel is Hack_Right de enige interventie die zich specifiek richt op het voorkomen van herhaald daderschap bij (jonge) cybercriminelen.

Ondanks dat er sprake is van een stijging van (het aantal aangiften van) cybercriminaliteit blijkt dit nog niet uit de instroom bij Hack_Right. Dit vraagt aanvullende analyse, opdat passende maatregelen kunnen worden ingezet. Daarom heeft het Ministerie van Justitie en Veiligheid voor de komende jaren subsidie toegezegd aan de drie uitvoeringsorganisaties (Reclassering, RvdK en Halt) voor de verdere implementatie en inbedding van Hack_Right in de justitiële processen. Daarnaast voert het WODC een onderzoek uit naar de in- en doorstroom van jeugdige en volwassen verdachten en daders van cybercrime binnen de strafrechtketen.[7]

Vraag 10
Komt het vaker voor dat er pas eindvonnis wordt gewezen door een rechtbank vier jaar nadat een verdachte in verzekering is gesteld? Zo ja, kunt u per rechtbank uitsplitsen hoe vaak de afgelopen vijf jaren vonnissen werden gewezen waarbij een dader strafvermindering kreeg als gevolg van schending van de redelijke termijn?

Antwoord op vraag 10
Het komt voor dat een rechtbank pas vier jaar nadat een verdachte in verzekering is gesteld het eindvonnis wijst. Uitsplitsen hoe vaak de afgelopen vijf jaren vonnissen zijn gewezen waarbij een dader strafvermindering kreeg als gevolg van schending van de redelijke termijn is niet geautomatiseerd mogelijk. Dit aangezien het overschrijden van de redelijke termijn niet wordt geregistreerd in de systemen van de rechtspraak.

Vraag 11
Indien uw antwoord op vraag 10 luidt dat nergens wordt geregistreerd of er sprake is van schending van de redelijke termijn en wat de gevolgen hiervan zijn voor de opgelegde straffen, kunt u dan een reële inschatting maken gebaseerd op de gepubliceerde uitspraken op rechtspraak.nl om de Kamer toch inhoudelijk van een antwoord te voorzien?

Antwoord op vraag 11
Het onderzoeken van gepubliceerde uitspraken op rechtspraak.nl is zeer tijdrovend en de huidige capaciteit laat het momenteel niet toe een dergelijk onderzoek uit te voeren. Bovendien worden (nu nog) lang niet alle uitspraken gepubliceerd. Daarom is het onduidelijk of een dergelijk onderzoek een representatief beeld zou geven.

[1] Tweakers, 22 februari 2022, Ddos'er die fiscus, banken en Tweakers aanviel, krijgt 200 uur taakstraf, https://tweakers.net/nieuws/193560/ddoser-die-fiscus-banken-en-tweakers-aanviel-krijgt-200-uur-taakstraf.html

[7] In- en doorstroom cyberdaders | Welk onderzoek doen we? | WODC - Wetenschappelijk Onderzoek- en Documentatiecentrum