ECLI:NL:HR:2021:1691

Instantie	Hoge Raad
Datum uitspraak	30-11-2021
Datum publicatie	30-11-2021
Zaaknummer	20/01564
Formele relaties	In cassatie op : ECLI:NL:GHSHE:2020:1514 Conclusie: ECLI:NL:PHR:2021:777
Rechtsgebieden	Strafrecht
Bijzondere kenmerken	Cassatie
Inhoudsindicatie	Computervredebreuk, art. 138ab Sr. 'Politiemol' die informatie uit politiesysteem doorspeelt aan criminelen. Wederrechtelijk binnendringen in geautomatiseerd werk m.b.v. valse sleutel en door aannemen van valse hoedanigheid. 1. Is verdachte m.b.v. 'valse sleutel' binnengedrongen? 2. Heeft verdachte 'valse hoedanigheid' aangenomen? Verdachte, die beschikte over een gebruikersnaam en wachtwoord voor toegang tot het beveiligde politiesysteem Blue View om i.h.k.v. zijn werk als politieambtenaar naspeuringen te verrichten, heeft het systeem bevraagd op gegevens over personen zonder dat daarvoor in de uitoefening van zijn politietaak enige aanleiding bestond. Hof heeft geoordeeld dat verdachte zijn autorisatie voor toegang tot Blue View heeft misbruikt om gegevens over criminelen in te zien, over te nemen en aan deze criminelen te verstrekken. Ad 1. 's Hofs op dit misbruik van de autorisatie gebaseerde oordeel dat verdachte m.b.v. een 'valse sleutel' a.b.i. art. 138ab.1.c Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, geeft mede in het licht van de totstandkomingsgeschiedenis van art. 138ab Sr niet blijk van een onjuiste rechtsopvatting en is niet onbegrijpelijk. Ad 2. 's Hofs oordeel dat verdachte aldus ook door het aannemen van een 'valse hoedanigheid' a.b.i. art. 138ab.1.c Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, kan niet z.m. uit de bewijsvoering worden afgeleid. De omstandigheid dat verdachte met het misbruik van zijn autorisatie het door zijn collega's en de maatschappij in hem gestelde vertrouwen heeft geschonden, volstaat daartoe niet. HR neemt daarbij in aanmerking dat niet blijkt dat verdachte al een valse hoedanigheid had aangenomen toen hem de autorisatie werd verstrekt. Dit leidt niet tot cassatie omdat de aard en ernst van het bewezenverklaarde in zijn geheel beschouwd niet worden aangetast door dit deel van bewezenverklaring weg te laten. Volgt verwerping. Samenhang met 20/01532 en 20/01547.
Vindplaatsen	Rechtspraak.nl SR-Updates.nl 2021-0360 NJB 2021/3271 RvdW 2021/1191 NJ 2022/54 met annotatie van J.M. ten Voorde

Uitspraak

HOGE RAAD DER NEDERLANDEN

STRAFKAMER

Nummer 20/01564

Datum 30 november 2021

ARREST

op het beroep in cassatie tegen een arrest van het gerechtshof 's-Hertogenbosch van 4 mei 2020, nummer 20-000736-18, in de strafzaak

tegen

[verdachte] ,

geboren te [geboorteplaats] op [geboortedatum] 1986,

hierna: de verdachte.

1 Procesverloop in cassatie

Het beroep is ingesteld door de verdachte. Namens deze hebben R.J. Baumgardt, P. van Dongen en S. van den Akker, allen advocaat te Rotterdam, bij schriftuur cassatiemiddelen voorgesteld. De schriftuur is aan dit arrest gehecht en maakt daarvan deel uit.

De advocaat-generaal T.N.B.M. Spronken heeft geconcludeerd tot vernietiging van de bestreden uitspraak maar uitsluitend wat betreft de opgelegde straf, tot vermindering daarvan en tot verwerping van het beroep voor het overige.

2 Beoordeling van het tweede cassatiemiddel

2.1 Het cassatiemiddel klaagt onder meer over het oordeel van het hof dat de verdachte met behulp van een valse sleutel en door het aannemen van een valse hoedanigheid het politiesysteem Blue View wederrechtelijk is binnengedrongen.

2.2.1 Overeenkomstig de tenlastelegging onder 2 is ten laste van de verdachte bewezenverklaard dat:

> "hij in de periode van 1 januari 2012 tot en met 29 september 2015 in Nederland telkens, opzettelijk en wederrechtelijk in een of meer (delen van) geautomatiseerde werken, namelijk in een of meer (delen van) servers van de politie en/of de belastingdienst, is binnengedrongen met behulp van een valse sleutel en door het aannemen van een valse hoedanigheid, namelijk door onbevoegd gebruik te maken van een gebruikersnaam en wachtwoord (voor de applicatie Blue View) en door zich met een gebruikersnaam en wachtwoord (voor de applicatie Blue View) toegang te verschaffen tot (delen van de) servers van de politie (waarop de applicaties Blue View en/of BVH en/of BVO en/of Summ-it en/of FIU waren geplaatst) met een ander doel dan waarvoor hem die gebruikersnaam en dat wachtwoord ter beschikking stonden en waarvoor hem die toegang was toegestaan, en (vervolgens) gegevens die waren opgeslagen en verwerkt en overgedragen door middel van (delen van) die geautomatiseerde werk(en) waarin hij zich wederrechtelijk bevond, voor zichzelf en anderen heeft overgenomen, namelijk door (telkens) (vertrouwelijke) informatie (omtrent een of meer personen en opsporingsonderzoeken) uit de

applicatie Blue View op (een) gegevensdrager(s) en/of in (een) document(en) te plaatsen en/of (naar zichzelf) te mailen en/of te exporteren en/of (vervolgens) aan daartoe niet-gerechtigde personen te verstrekken."

2.2.2 Het hof heeft ten aanzien van de bewezenverklaring onder meer overwogen:

"De loopbaan van verdachte bij de politie
Verdachte is op 26 januari 2009 aangesteld als aspirant in tijdelijke dienst gedurende de initiële opleiding (zes jaar) bij de Dienst Nationale Recherche (hierna: DNR). Hij is een zij-instromer op niveau 4. Op 21 november 2008 tekende verdachte daartoe een geheimhoudersverklaring van de Landelijke Eenheid en op 15 december 2008 werd een verklaring van geen bezwaar voor deze functie afgegeven. Op 22 april 2009 legde verdachte de ambtseed af en ondertekende hij het eedsformulier.

Op 13 juli 2010 werd verdachte aangesteld als generalist tactische recherche tot en met 31 juli 2011 en op 28 juli 2011 werd de proeftijd verlengd tot en met 31 januari 2012. Op 1 februari 2012 volgde een vaste aanstelling bij de DNR.

Op 14 oktober 2011 ontving het hoofd van het Bureau Veiligheid en Integriteit KLPD een brief 'Weigering verklaring van geen bezwaar' (hierna: VGB) met betrekking tot verdachte, waarin wordt vermeld dat verdachte van deze weigering op de hoogte is gesteld.

Door deze weigering kon verdachte niet bij de DNR blijven werken en werd hij op verschillende locaties tewerkgesteld. Hij werkte onder andere in 2013 bij de Dienst Verkeer van het KLPD in Driebergen in Maasbracht en in 2014 bij de Landelijk Eenheid, Dienst Infra, locatie Croeselaan te Utrecht. Daarnaast werkte hij nog in de regio Venlo en Eindhoven ten behoeve van het behalen van modules in het kader van zijn opleiding.

(...)

Blue View

Blue View is een indexsysteem, waarin dumps plaatsvinden van diverse politiesystemen, zoals BVO, Summ-it, HKS, BVH, Luris, FIU, afkomstig van bijna alle opsporingsinstanties van Nederland (Kmar, FIOD et cetera).

Accounts in Blue View zijn strikt persoonlijk en mogen niet gedeeld worden.

Om Blue View te raadplegen wordt ingelogd met een gebruikersnaam en een wachtwoord. De gebruikersnaam is het dienstnummer van de verbalisant, [001] , zijnde verdachte. Hij had een Blue View account vanaf 29 augustus 2011 om 10.18 uur, op niveau Opsporing basis 3 en 4. Bevragingen geschieden op een zogenaamde lange KENO, een zoeksleutel gebaseerd op onder andere achternaam en geboortejaar van de te bevragen persoon. Resultaten van bevragingen kunnen worden geëxporteerd als PDF- of Excelbestand. Vervolgens kunnen deze worden opgeslagen op bijvoorbeeld een harde schijf van een computer of op een USB-stick, indien de gebruiker rechten heeft om gegevens op een USB-stick op te slaan. Verdachte had die rechten. In de naam die het document krijgt tijdens het exporteren zit de tekst 'Registratie Export'. Uit de bestandsnaam is af te leiden op welke datum de export is gemaakt en wat het accountnummer is van de gebruiker.

Op het eerste blad van elke export is een waarschuwing opgenomen voor de gebruiker:

'Het oneigenlijk gebruik dan wel misbruik van deze gegevens is ten strengste verboden. Daarnaast is het verstrekken van deze gegevens aan derden welke niet de vereiste autorisatie bezitten eveneens ten strengste verboden'. De gebruiker kan pas verder gaan met exporteren als hij aangeeft dat hij de bovenstaande waarschuwing heeft gelezen en op OK drukt.

(...)

Voorts is door de verdediging aangevoerd dat de 28.521 logregels in Blue View niet representatief zijn voor het aantal zoekopdrachten, nu elke mutatie in Blue View een nieuwe logregel creëert. Verdachte schat zelf dat hij ongeveer 5000 bevragingen heeft uitgevoerd. Ter

onderbouwing van dit verweer heeft de verdediging het navolgende naar voren gebracht.

a. Verdachte heeft bij de rechter-commissaris en ter zitting in eerste aanleg en hoger beroep aangevoerd dat niet kan worden aangenomen dat alle bevragingen in die periode illegaal werden gedaan. Hij werd immers, ook nadat hij niet meer bij de DNR werkzaam was, juist speciaal in onderzoeken ingezet met de vraag om gebruik te maken van zijn accreditatie voor Blue View en ook omdat hij een zekere handigheid had in het bevragen van dat systeem.

b. (...)

Het hof overweegt, samen met de rechtbank, met betrekking tot deze stellingen van verdachte het volgende:

a. Dat verdachte wel eens door collega's zou zijn benaderd om Blue View te bevragen wordt ook door de getuigen [betrokkene 2] en [betrokkene 3] bij de rechter-commissaris niet ontkend, zij het dat zij hem zelf nooit gevraagd hebben Blue View te raadplegen. Het hof sluit dan ook niet uit dat het heel wel kan zijn dat verdachte op verzoek wel eens ten behoeve van opsporingsonderzoeken Blue View heeft bevraagd, ook nadat hij niet meer bij de DNR werkzaam was. Hij had immers zijn accreditatie op niveau 3 en 4 gewoon behouden. Gelet op de enorme hoeveelheid gevoelige informatie die door verdachte is bevraagd, welke niet allemaal volledig is onderzocht, is het niet uit te sluiten dat verdachte op verzoek van collega's daadwerkelijk wel eens informatie uit het systeem heeft opgevraagd. Door verdachte is overigens geen enkel voorbeeld aangewezen waarbij dat het geval zou zijn geweest. Het hof is echter van oordeel, dat dit onverlet laat dat door verdachte zonder enige professionele aanleiding of intern verzoek ook grote hoeveelheden vertrouwelijke informatie zijn bevraagd en geëxporteerd die aangetroffen zijn bij derden zoals het hof hierna nog zal bespreken. Wat er ook zij van het verweer, het staat een bewezenverklaring niet in de weg. Het verweer faalt daarom reeds in zoverre.

(...)

Met betrekking tot feit 2: computervredebreuk

De advocaat-generaal stelt zich op het standpunt dat dit feit bewezen kan worden verklaard.

Door de verdediging is vrijspraak bepleit. Daartoe heeft zij - kort gezegd - het volgende aangevoerd. Er is geen sprake van het zogenaamd ‘hacken’ zoals bedoeld in artikel 138ab Wetboek van Strafrecht. De rechtbank heeft het begrip ‘binnendringen’ verkeerd uitgelegd. Dit artikel strekt namelijk niet tot de bescherming van de (inhoud van) gegevens, maar is bedoeld om het binnendringen op zich strafbaar te stellen. Dit blijkt des te meer uit het nieuwe artikel 138c Wetboek van Strafrecht, in welk artikel het met rechtmatig toegang wederrechtelijk overnemen van gegevens strafbaar is gesteld. Van dergelijk binnendringen is thans geen sprake, nu verdachte beschikte over een rechtmatige 'sleutel', te weten zijn accreditatie om Blue View te raadplegen. Bovendien is geen sprake van een valse hoedanigheid, doorbreken van beveiliging of technische ingreep van de zijde van verdachte, aldus de verdediging.

Het hof stelt, onder verwijzing naar artikel 80sexies Sr zoals geldend ten tijde van het tenlastegelegde, samen met de rechtbank vast dat - zoals bij de bespreking van feit 1 aan de orde is geweest - het Blue View systeem een geautomatiseerd werk is, in casu zijnde een digitaal verzamelsysteem dat door politieambtenaren in de uitoefening van hun politietaak kan worden geraadpleegd mits zij daarvoor zijn geaccrediteerd en beschikken over een autorisatie. Er moeten om in het beveiligde systeem te komen een gebruikersnaam (dienstnummer) en wachtwoord worden gegeven. Verdachte beschikte over een zodanige autorisatie vanaf 29 augustus 2011 tot zijn aanhouding op 29 september 2015.

Het hof overweegt omtrent het verweer dat verdachte rechtmatig beschikte over een autorisatie waarmee hij Blue View kon raadplegen en dat daarmee geen veroordeling ter zake van het onder

2 tenlastegelegde kan volgen, als volgt.

(...)

Het schenden van artikel 138ab Sr was tot de inwerkingtreding van de Wet kraken en leegstand (Stb. 2010, 320) tot 1 oktober 2010 geregeld in art. 138a Sr. Op grond van de parlementaire stukken kan ter zake van het huidige art. 138ab Sr - het toenmalige art. 138a Sr - het volgende worden opgemerkt.

De strafbaarstelling van art. 138ab Sr beschermt degene die blijkens feitelijke beveiliging heeft duidelijk gemaakt dat hij zijn gegevens heeft willen afschermen tegen nieuwsgierige blikken door het systeem daartegen te beveiligen. De bescherming van gerechtvaardigde belangen van houders van gegevensbestanden die, opgeslagen in computers, vooral via de telecommunicatie-infrastructuur voor onbevoegde blikken toegankelijk zijn, wordt via deze strafbaarstelling geboden doordat het doorbreken van een aangebrachte beveiliging wordt strafbaar gesteld. Daarbij is aansluiting gezocht bij de bestaande strafbaarstelling betreffende de huisvredebreuk. De eisen rondom wederrechtelijke binnendringing zijn in de sfeer van de informatietechniek in deze strafbaarstelling vertaald in het bestanddeel 'binnendringen', inhoudende dat een beveiliging moet zijn doorbroken. In de Memorie van Toelichting is hierover opgenomen: 'Het gaat er om dat degeen die de computer binnendringt door het doorbreken van de beveiliging, heeft blijk gegeven de wetenschap te hebben gehad dat hij een beveiligd systeem binnendringt en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken' (vgl. Kamerstukken II 1989/90, 21 551, nr. 3, p. 16).

Het aangehaalde lid 1 van artikel 138ab Sr geeft aan dat van 'binnendringen' in ieder geval sprake is indien de toegang tot het werk wordt verworven met behulp van een valse sleutel of door het aannemen van een valse hoedanigheid. In de Kamerstukken van het toenmalige wetsvoorstel wordt over het bestanddeel 'valse sleutel' weergegeven dat een password een sleutel is die de gebruiker toegang geeft tot het systeem of tot een deel daarvan. Daarbij werd aangehaald dat de Hoge Raad in zijn arrest van 20 mei 1986, ECLI:NL:HR:1986:AC9359, NJ 1987/130, heeft bepaald dat een huissleutel die wordt gebruikt tot opening van een slot door iemand die daartoe niet is gerechtigd, een valse sleutel is en dat niet is vereist dat ten aanzien van de sleutel enige beveiligingsmaatregel is genomen. Onder verwijzing naar artikel 90 Sr, waarin geen definitie van het begrip 'valse sleutels' wordt gegeven maar enkel wordt aangegeven wat onder het begrip dient te worden begrepen ('alle tot opening van het slot niet bestemde werktuigen') - waarbij de wetgever heeft aangegeven dat "(O)nverschillig (is) of het werktuig al of niet een sleutel is, zoo het slechts niet die sleutel is, die voor opening van dat slot bestemd is." (zie H.J. Smidt, Geschiedenis van het Wetboek van Strafrecht, Deel I, tweede druk, p. 544) - stelt het hof dat de jurisprudentie van de Hoge Raad verder ter zake van 'valse sleutel' heeft uitgemaakt dat ook onrechtmatig gebruik van bijvoorbeeld een bankpas of een tankpas kan worden aangemerkt als het gebruik maken van een 'valse sleutel'. Anders gezegd: de Hoge Raad geeft een ruime uitleg aan het begrip 'valse sleutels' waarbij ook gebruik door een onbevoegde als een 'valse sleutel' kan worden aangemerkt (vgl. CAG Knigge in ECLI:NL:PHR:2017:1012 onder verwijzing naar HR 3 oktober 2017, ECLI:NL:HR:2017:2546).

Voor wat betreft de uitleg in de genoemde bepaling ter zake van het bestanddeel 'valse hoedanigheid' wijst het hof op de uitleg die de Hoge Raad daaraan geeft in zijn overzichtsarrest van 20 december 2016, ECLI:NL:HR:2016:2892, NJ 2017/158, m.nt. Keijzer, rov. 2.3.4. De Hoge Raad heeft ter zake van het aannemen van een valse hoedanigheid overwogen dat het daarbij in de kern erom gaat dat het handelen van de verdachte ertoe kan leiden dat bij de ander een onjuiste voorstelling van zaken in het leven wordt geroepen met betrekking tot de 'persoon' van de verdachte wat betreft diens hoedanigheid, waarbij die onjuiste voorstelling van zaken in het leven wordt geroepen teneinde daarvan misbruik te maken. Daarbij heeft de Hoge Raad specifiek aangegeven dat de in de rechtspraak wel gebruikte formulering dat een verdachte zich als een 'bonafide' deelnemer aan het rechtsverkeer heeft gepresenteerd, met betrekking tot het aannemen van een valse hoedanigheid slechts relevant is als zo een presentatie als bonafide

(potentiële) wederpartij berust op voldoende specifieke gedragingen die in de desbetreffende context erop zijn gericht bij het beoogde slachtoffer een onjuiste voorstelling van zaken in het leven te roepen teneinde daarvan misbruik te maken.

De verdachte heeft op enig moment, namelijk toen hij werkzaam zou worden bij de Nationale Recherche toegang gekregen tot het beveiligde Blue View systeem. Om Blue View te kunnen raadplegen, heeft verdachte moeten inloggen met een gebruikersnaam (zijn dienstnummer) en een wachtwoord. Daarmee verkreeg verdachte ook de bevoegdheid om de resultaten van bevragingen te kunnen exporteren als PDF of Excel-bestand en op te slaan op bijvoorbeeld een externe opslagplaats, zoals een USB stick. Verdachte werd daarbij uitdrukkelijk via het systeem gewaarschuwd dat oneigenlijk gebruik dan wel misbruik van deze gegevens, waaronder het verstrekken van deze gegevens aan derden welke niet de vereiste autorisatie bezitten, ten strengste verboden was. Zoals hierboven weergegeven zijn deze werkzaamheden spoedig gestaakt omdat hij geen “Verklaring van geen bezwaar” verkreeg. Desalniettemin heeft verdachte nog jaren dit systeem ingezien.

Het hof oordeelt dat verdachte op grond van de in het voorgaande weergegeven feiten en omstandigheden het beveiligde politiesysteem Blue View, dat hij in het kader van zijn specifieke werkzaamheden als politieambtenaar op die betreffende gegevens niet behoefde en niet behoorde in te zien, heeft misbruikt om informatie/gegevens over criminelen in te zien, deze informatie/gegevens over te nemen en deze informatie/gegevens ook aan deze criminelen te verstrekken. Hij is met behulp van de aan hem toegekende autorisatie het systeem Blue View opzettelijk en wederrechtelijk binnengedrongen om inzage te krijgen van gegevens waar hij niet toe bevoegd was en vervolgens deze over te nemen. Door op deze wijze de betreffende gegevens in te zien en over te nemen, heeft verdachte, wetende dat het een beveiligd systeem betrof, doelbewust de beveiliging van dit systeem doorbroken en is hij derhalve het systeem binnengedrongen. Hij heeft zich daarbij bediend van een valse sleutel en het aannemen van een valse hoedanigheid. Verdachte heeft immers weliswaar geautoriseerd maar onbevoegd ter zake van de betreffende gegevens zich opzettelijk en wederrechtelijk de toegang verschaft tot het systeem Blue View. Daarbij was aan verdachte de autorisatie verstrekt om het systeem te raadplegen om in het kader van zijn werk als politieambtenaar naspeuringen te verrichten, maar niet om daarmee informatie in te winnen en dit aan criminelen te verstrekken waardoor dezen zich aan die naspeuringen konden onttrekken. Tevens heeft verdachte in de context van zijn handelen als politieambtenaar voldoende specifieke gedragingen verricht om een onjuiste voorstelling van zaken in het leven te roepen met betrekking tot de hoedanigheid van de 'persoon' van de verdachte. Verdachte heeft namelijk onder de voorstelling van de hoedanigheid van een persoon die gerechtigd was om op grond van zijn werkzaamheden inzage in de betreffende gegevens te mogen verrichten, zich de toegang verschaft tot het systeem Blue View, teneinde daarvan misbruik te maken. Verdachte bevroeg vele personen in het Blue View systeem zonder dat is gebleken dat daartoe in de uitoefening van zijn politietaak enige aanleiding bestond. Zowel de collega’s van verdachte als de maatschappij mocht erop vertrouwen - mede gelet op de aard en de functie van verdachte en de ambtseed die hij heeft moeten afleggen - dat zij te maken hadden met een betrouwbare en onkreukbare ambtenaar. Verdachte heeft echter op bedrieglijke wijze misbruik gemaakt van het vertrouwen van en in de politie.

Anders dan de verdediging is het hof van mening dat de strafbaarstelling opgenomen in artikel 138c Sr geen inbreuk maakt op een mogelijke bewezenverklaring van hetgeen aan verdachte onder 2 is tenlastegelegd en strafbaar is gesteld onder artikel 138ab Sr. De wetgever heeft in artikel 138c Sr strafbaar gesteld het opzettelijk en wederrechtelijk voor zichzelf of voor een ander overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk. De bepaling is vooral van belang voor gevallen waarin de dader rechtmatige toegang heeft tot de gegevens, maar deze wederrechtelijk overneemt (vgl. Kamerstukken II 2015/16, 34 372, nr. 3, p. 64). In de onderhavige zaak had verdachte weliswaar autorisatie om toegang te krijgen tot het systeem Blue View, maar hij was niet

bevoegd tot het inzien en overnemen van de gegevens waar het in de onderhavige strafzaak om gaat. Verdachte heeft derhalve met behulp van de aan hem toegekende autorisatie het systeem Blue View opzettelijk en wederrechtelijk binnengedrongen om inzage te krijgen van gegevens waar hij niet toe bevoegd was en vervolgens deze overgenomen.

Het hof is dan ook van oordeel dat de tenlastegelegde computervredebreuk bewezen kan worden verklaard."

2.3.1 De tenlastelegging is toegesneden op artikel 138ab van het Wetboek van Strafrecht (hierna: Sr). Daarom moet worden aangenomen dat de in de tenlastelegging en de bewezenverklaring voorkomende begrippen "wederrechtelijk binnengedrongen", "valse sleutel" en "valse hoedanigheid" zijn gebruikt in de betekenis die deze begrippen hebben in die bepaling.

2.3.2 Artikel 138ab lid 1 en 2 Sr zoals dat gold vanaf 1 oktober 2010 - en dat op het aan de orde zijnde punt niet verschilt van de nu geldende tekst - luidde:

"1. Met gevangenisstraf (...) wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
a. door het doorbreken van een beveiliging,
b. door een technische ingreep,
c. met behulp van valse signalen of een valse sleutel, of
d. door het aannemen van een valse hoedanigheid.
2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt."

2.3.3 De strafbaarstelling van computervredebreuk was tot 1 oktober 2010 opgenomen in artikel 138a (oud) Sr. Deze bepaling is ingevoerd bij Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit), Stb. 1993, 93. Volgens de memorie van toelichting geeft het wetsvoorstel uitvoering aan het rapport 'Informatietechniek en strafrecht' van de Commissie computercriminaliteit (Commissie Franken). In dat rapport is ten aanzien van de voorgestelde strafbaarstelling van computervredebreuk onder meer het volgende vermeld (p. 59-60):

"98 (...) Van 'binnendringen' is sprake (zo is althans de opvatting ten aanzien van de term in artikel 138 Sr) indien men zich de toegang verschaft tegen de onmiskenbare wil van de rechthebbende, welke zowel uit woorden als daden kan blijken. In het eerste geval zou voor strafbaarheid van het pogen de toegang te verkrijgen tot informatietechnische systemen een tekst 'verboden toegang voor onbevoegden' volstaan (maar: zie 100). In het tweede geval zou een duidelijke drempel moeten bestaan zodat onbevoegden zich niet simpelweg toegang kunnen verschaffen. Men denke hier aan wachtwoorden, PIN-codes en dergelijke: indien gebruik daarvan nodig is om toegang te krijgen, openbaart zich daarmee de wil van de rechthebbenden onbevoegden de toegang te weigeren.

99 Een inperking geeft de toevoeging van de term 'wederrechtelijk'. Of zich wederrechtelijkheid voordoet, zou moeten worden vastgesteld in het licht van de verhouding tussen degene die binnendringt en degene in wiens systeem wordt binnengedrongen. Daarbij speelt een rol of er duidelijke afspraken zijn, en of sprake is van (ongeschreven) regels in het maatschappelijk verkeer.

Zo kan men zich afvragen of van wederrechtelijk binnendringen bijvoorbeeld ook sprake is wanneer een persoon die werkzaam is in een bedrijf of instelling en aan wie door de leiding de bevoegdheid is gegeven om alleen bestaande delen van het gegevensverwerkend systeem te benaderen, binnendringt in andere niet voor hem opengestelde delen. De commissie meent dat de jurisprudentie rond het bestanddeel 'wederrechtelijk binnendringen' in artikel 138 Sr leert dat deze term ook in dit verband in zich voordoende gevallen een voldoende onderscheidend

vermogen zal hebben om te bepalen wat wel en wat niet als strafbaar moet worden aangemerkt. Tevens leert die jurisprudentie betreffende artikel 138 Sr dat de praktijk dermate verscheiden is dat het a priori pogen te vinden van nadere criteria waarschijnlijk een onbevredigend resultaat geeft - een dergelijke verscheidenheid zal immers ook bij computervredebreuk aanwezig zijn.

Duidelijk is wel dat de 'hacker', die van buitenaf (dat wil zeggen via de openbare telecommunicatie-infrastructuur) beveiligde systemen binnendringt zonder meer onder de werking van de voorgestelde bepaling zal vallen.

100 Met betrekking tot de zinsnede "een daartegen beveiligd werk" wordt het volgende opgemerkt. In alinea 98 is betoogd dat van binnendringen sprake is, indien men zich toegang verschaft tegen de onmiskenbare wil van de rechthebbende -deze wil zou kunnen blijken uit woorden ("verboden toegang") of uit daden. De commissie meent dat woorden alleen niet voldoende zijn. Woorden, bijvoorbeeld de tekst op het beeldscherm dat toegang voor onbevoegden verboden is, geven wel onmiskenbaar een wil van de rechthebbende weer, doch sluiten toegang per ongeluk niet uit. Dit gevaar is in veel mindere mate aanwezig bij een hogere drempel, bestaande uit bepaalde, tegen het wederrechtelijk binnendringen gerichte, beveiligingsmaatregelen. Hiermee is een nadere inperking aangebracht. De deur moet als het ware niet alleen dicht zijn, maar ook op slot.

101 In het tweede lid staat een -niet limitatieve- opsomming van manieren waarop onbevoegd toegang kan zijn verkregen, wil van binnendringen sprake zijn. De formulering is zo dat diverse manieren om toegangsbeveiligingen te doorbreken, dan wel te omzeilen, er onder te brengen zijn.

Gesproken wordt van een 'valse hoedanigheid', 'listige kunstgrepen' (conform artikel 326 Sr) en van een 'valse sleutel' (conform artikel 90 Sr). De commissie beoogt daarmee die situaties onder de werking van de strafbepaling te brengen, waarin men de beschikking heeft verkregen over overigens geldige toegangsmiddelen, echter zonder toestemming van de beheerder van de inrichting of de houder van de toegangsmiddelen.

(...)

De termen 'valse hoedanigheid' en 'valse sleutel' zien op het gebruik van niet legaal verkregen toegangsmiddelen. Degene die een magneetpas of een toegangscode van een ander zonder diens toestemming gebruikt, hult zich in de valse hoedanigheid van de bevoegde gebruiker of maakt gebruik van een valse sleutel, wanneer de toegangsprocedure niet in een identificatie doch slechts in een autorisatie van de gebruiker voorziet."

2.3.4 De memorie van antwoord aan de Tweede Kamer bij het wetsvoorstel dat heeft geleid tot de Wet computercriminaliteit houdt ten aanzien van het voorgestelde artikel 138a Sr onder meer het volgende in:

"Ingevolge de nieuw in de nota van wijziging voorgestelde bepaling is al sprake van strafbaarheid indien de toegang is verkregen door listige kunstgrepen, een valse sleutel of het aannemen van een valse hoedanigheid. Ik ga er daarbij vanuit dat een password een sleutel is die de gebruiker toegang geeft tot het systeem of tot een deel daarvan."

(Kamerstukken II 1990/91, 21551, nr. 6, p. 31)

2.4.1 Het hof heeft vastgesteld, kort gezegd, dat de verdachte als politieambtenaar voorafgaand aan de bewezenverklaarde periode een autorisatie heeft verkregen voor toegang tot het beveiligde politiesysteem Blue View, waartoe hij de beschikking had over een gebruikersnaam (zijn dienstnummer) en een wachtwoord. Verder heeft het hof vastgesteld dat die autorisatie aan de verdachte was verstrekt om in het kader van zijn werk als politieambtenaar naspeuringen te verrichten, maar dat de verdachte het systeem vervolgens heeft bevraagd op gegevens over personen zonder dat daarvoor in de uitoefening van zijn politietaak enige aanleiding bestond. Op die manier kreeg de verdachte zonder daartoe bevoegd te zijn inzage in gegevens en nam hij deze gegevens over. Op grond hiervan heeft het hof geoordeeld dat de verdachte zijn autorisatie voor toegang tot het systeem Blue View heeft "misbruikt om informatie/gegevens over

criminelen in te zien, deze informatie/gegevens over te nemen en deze informatie/gegevens ook aan deze criminelen te verstrekken".

2.4.2 Het op dit misbruik van die autorisatie gebaseerde oordeel van het hof dat de verdachte met behulp van een "valse sleutel" als bedoeld in artikel 138ab lid 1, onder c, Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, geeft mede in het licht van de onder 2.3.3 en 2.3.4 weergegeven totstandkomingsgeschiedenis van (het huidige) artikel 138ab Sr niet blijk van een onjuiste rechtsopvatting. Dat oordeel is ook niet onbegrijpelijk.

2.4.3 Het oordeel van het hof dat de verdachte aldus ook door het aannemen van een "valse hoedanigheid" als bedoeld in artikel 138ab lid 1, onder d, Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, kan echter niet zonder meer uit de bewijsvoering worden afgeleid. De door het hof in aanmerking genomen omstandigheid dat de verdachte met het misbruik van zijn autorisatie het door zijn collega's en de maatschappij in hem gestelde vertrouwen heeft geschonden, volstaat daartoe niet. De Hoge Raad neemt daarbij in aanmerking dat niet blijkt dat de verdachte al een valse hoedanigheid had aangenomen toen hem de autorisatie werd verstrekt. Het slagen van de hierop gerichte klacht leidt echter, mede gelet op wat onder 2.4.2 is overwogen, niet tot cassatie omdat het weglaten van dit deel van de bewezenverklaring de aard en de ernst van het bewezenverklaarde in zijn geheel beschouwd niet aantast.

2.5 Het cassatiemiddel is tevergeefs voorgesteld.

3 Beoordeling van de cassatiemiddelen voor het overige

De Hoge Raad heeft ook de overige klachten over de uitspraak van het hof beoordeeld. De uitkomst hiervan is dat ook deze klachten niet kunnen leiden tot vernietiging van die uitspraak. De Hoge Raad hoeft niet te motiveren waarom hij tot dit oordeel is gekomen. Bij de beoordeling van deze klachten is het namelijk niet nodig om antwoord te geven op vragen die van belang zijn voor de eenheid of de ontwikkeling van het recht (zie artikel 81 lid 1 van de Wet op de rechterlijke organisatie).

4 Ambtshalve beoordeling van de uitspraak van het hof

De verdachte bevindt zich in voorlopige hechtenis. De Hoge Raad doet uitspraak nadat meer dan zestien maanden zijn verstreken na het instellen van het cassatieberoep. Dat brengt mee dat de redelijke termijn als bedoeld in artikel 6 lid 1 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden is overschreden. Dit moet leiden tot vermindering van de opgelegde gevangenisstraf van vijf jaren.

5 Beslissing

De Hoge Raad:

- vernietigt de uitspraak van het hof , maar uitsluitend wat betreft de duur van de opgelegde gevangenisstraf;

- vermindert deze in die zin dat deze vier jaren en tien maanden beloopt;

- verwerpt het beroep voor het overige.

Dit arrest is gewezen door de vice-president V. van den Brink als voorzitter, en de raadsheren Y. Buruma en T. Kooijmans, in bijzijn van de waarnemend griffier H.J.S. Kea, en uitgesproken ter openbare terechtzitting van 30 november 2021.