LJN: BN9287, Hoge Raad , 09/02184

Datum uitspraak: 22-02-2011

Datum publicatie: 22-02-2011

Rechtsgebied: Straf

Soort procedure: Cassatie

Inhoudsindicatie: Computercriminaliteit. Verdachte en OM in cassatie. 1. Verwerping verweer dat geen sprake kan zijn van overtreding van art. 138a (oud) Sr. 2. Onjuiste uitleg Hof van de in de tenlastelegging opgenomen bestanddelen ‘geautomatiseerd werk’ en ‘gemeen gevaar voor de verlening van diensten’. Ad 1. Het Hof heeft geoordeeld dat elke consumentenversie van het computerbesturingssysteem Windows XP is voorzien van enige beveiliging in de zin van art. 138a.1 aanhef en onder a (oud) Sr. Dat oordeel geeft geen blijk van een onjuiste rechtsopvatting en is niet onbegrijpelijk. Opmerking verdient daarbij dat onder het doorbreken van enige beveiliging mede dient te worden verstaan het tegen de wil van de rechthebbende binnendringen in een computer langs een weg die de aanwezige beveiliging niet of onvoldoende afsluit. Daarbij is niet van belang of die opening inherent is aan het systeem of is veroorzaakt door andere ‘aanvallers’. Voor zover het middel opkomt tegen de verwerping van het verweer dat geen sprake is van een technische ingreep met de klacht dat dit niet uit de bewijsmiddelen kan worden afgeleid, berust het op een onjuiste lezing van ’s Hofs arrest. Het oordeel van het Hof moet aldus worden verstaan dat het als de bedoelde technische ingreep heeft aangemerkt het samenstel van alle handelingen die nodig waren voor de verspreiding van het virus. Dat oordeel geeft geen blijk van een onjuiste rechtsopvatting en is niet onbegrijpelijk. Ad 2. In art. 161sexies, aanhef en onder 2°, (oud) Sr wordt wat betreft de term ‘geautomatiseerd werk’ geen onderscheid gemaakt tussen computers van dienstverlenende instellingen en computers van afnemers van diensten. Ook in de wetsgeschiedenis wordt dat onderscheid niet gemaakt. Blijkens de hiervoor weergegeven onderdelen van die wetsgeschiedenis beoogde de wetgever met de invoering van deze bepaling onder meer strafrechtelijke bescherming te verlenen aan het belang van de verlening van diensten, voor zover deze in gevaar gebracht kan worden door onder meer het opzettelijk veroorzaken van een stoornis in de werking van een geautomatiseerd werk. Onder het begrip geautomatiseerd werk dienen ook computers en netwerken van aan elkaar verbonden computers te worden begrepen, terwijl in het verlengde daarvan op grond van de door de wetgever voorgestane dynamische wetsuitleg daarbij tegenwoordig ook moet worden gedacht aan, zoals i.c., een reeks van computers die door middel van schadelijke, via het internet verspreide software met elkaar zijn verbonden. Onder ‘gemeen gevaar’ dient in dit verband mede te worden verstaan het gevaar voor een ongestoorde dienstverlening aan een onbestemd doch aanmerkelijk aantal afnemers. Uit een en ander moet worden afgeleid dat voor de beantwoording van de vraag of een stoornis is veroorzaakt in een geautomatiseerd werk en of daarvan gemeen gevaar voor de verlening van diensten te duchten is geweest, zoals bedoeld in art. 161sexies, aanhef en onder 2° (oud), Sr, niet van doorslaggevende betekenis is of die stoornis wordt veroorzaakt in de computers van de afnemers van een dienst, ook als die door een netwerk aan elkaar zijn verbonden, dan wel van dergelijke computers van de dienstverlener, maar dat het erom gaat of van de opzettelijk veroorzaakte stoornis gemeen gevaar te duchten was voor een ongestoorde dienstverlening. Het Hof heeft geoordeeld dat de wetgever met de strafbaarstelling van art. 161sexies, aanhef en onder 2°, Sr kennelijk de strafrechtelijke bescherming van geautomatiseerde werken die gemeen/ten algemene nutte worden gebruikt, voor ogen heeft gehad en heeft aan het bewijs van het te duchten gemeen gevaar voor de verlening van diensten de voorwaarde verbonden dat een storing is veroorzaakt in geautomatiseerde werken van de betreffende bancaire instellingen of creditcardmaatschappijen zelf. Het Hof heeft daarbij kennelijk onderscheid gemaakt tussen de computers van afnemers van een dienst en de computers van de dienstverlener, in die zin dat een stoornis in de computers van de afnemers niet het bedoelde te duchten gemeen gevaar voor de verlening van diensten kan opleveren. Daarmee heeft het Hof het hiervoor overwogene miskend en heeft het aan de vrijspraak van verdachte van de onder 2 en 3 tenlastegelegde feiten een onjuiste rechtsopvatting ten grondslag gelegd.

Uitspraak
22 februari 2011
Strafkamer
nr. 09/02184

Hoge Raad der Nederlanden

Arrest

op het beroep in cassatie tegen een arrest van het Gerechtshof te 's-Hertogenbosch van 12 september 2008, nummer 20/000628-07, in de strafzaak tegen:
[Verdachte], geboren te [geboorteplaats] op [geboortedatum] 1986, wonende te [woonplaats].

1. Geding in cassatie

1.1. De beroepen zijn ingesteld door de verdachte en de Advocaat-Generaal bij het Hof. Namens de verdachte heeft mr. S.B.J. Hiemstra, advocaat te Haarlem, bij schriftuur een middel van cassatie voorgesteld. De schriftuur is aan dit arrest gehecht en maakt daarvan deel uit.
De Advocaat-Generaal bij het Hof heeft bij schriftuur een middel van cassatie voorgesteld. De schriftuur is aan dit arrest gehecht en maakt daarvan deel uit.
De Advocaat-Generaal Knigge heeft geconcludeerd tot vernietiging van de bestreden uitspraak, doch uitsluitend wat betreft de opgelegde straf, tot vermindering daarvan en tot verwerping van de beroepen voor het overige.

1.2. De raadsman heeft schriftelijk op de conclusie gereageerd.

2. Beoordeling van het namens de verdachte voorgestelde middel

2.1. Het middel komt op tegen de verwerping van het verweer dat geen sprake kan zijn van overtreding van art. 138a (oud) Sr, zoals aan de verdachte onder 1 is tenlastegelegd, omdat geen beveiliging is doorbroken en omdat geen technische ingreep heeft plaatsgevonden.

2.2.1. Ten laste van de verdachte is onder 1 bewezenverklaard dat:
"hij op tijdstippen in de periode van 1 juni 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met een ander, telkens opzettelijk wederrechtelijk in een geautomatiseerd werk voor de opslag of verwerking van gegevens, te weten computers, is binnengedrongen, waarbij hij, verdachte en zijn medeverdachte de beveiliging hebben doorbroken, in elk geval de toegang hebben verworven door een technische ingreep, met behulp van valse signalen en/of door het aannemen van een valse hoedanigheid, namelijk telkens door, gebruikmakend van één of meer kwetsbaarheden in het besturingssysteem van Windows, een (al dan niet door verdachte gemaakte/ontwikkelde) versie van een virus, onder meer bekend onder de naam Toxbot, te (doen) verspreiden en/of te (doen) installeren waarna hij, verdachte en zijn mededader, door tussenkomst van het geautomatiseerde werk waarin zij zijn binnengedrongen de toegang hebben verworven tot geautomatiseerde werken van derden".

2.2.2. Het Hof heeft het in het middel bedoelde verweer als volgt samengevat en verworpen:
"D1.
Zijdens verdachte is door de raadsman ter terechtzitting in hoger beroep bepleit dat verdachte wordt vrijgesproken van het onder 1 ten laste gelegde nu niet bewezen kan worden dat een (minimale) beveiliging is doorbroken dan wel dat een technische ingreep gepleegd is door verdachte en/of zijn medeverdachte, zoals, aldus de verdediging, vereist op grond van artikel 138a van het Wetboek van Strafrecht.
D2.
Het hof overweegt hiertoe het volgende.
Op grond van het verhandelde ter terechtzitting in hoger beroep stelt het hof onder meer het volgende vast.
(bijlage A000:)
a. Op 31 mei 2005 wordt door de Security Manager van het reken- en netwerkdienstencentrum genaamd SARA aangifte gedaan terzake computervredebreuk (bijlage 2 van bijlage A000).
b. Getuige [getuige 1] bleek een bestand met alle beheerderswachtwoorden van de computersystemen waarover SARA het beheer heeft, te hebben ontvangen van verdachte (bijlage 3 van bijlage A000).
(bijlage A001:)
c. Verdachte (Het hof: zichzelf ook wel [verdachte] noemend) vertelt in een chatsessie van 25 mei 2005 met [getuige 1] (het hof: zichzelf [getuige 1] noemend) dat hij beschikt over een botnet.
d. Uit een chatsessie van 12 april 2005 met [getuige 1] blijkt dat [verdachte] beschikt over de domeinnamen devtech.us, randomized.it, memzero.info, lsass.org, lsass.com, lsass.cc en devnologie.info.
e. Op de website van de antivirusmaatschappij Symantec staat een beschrijving van een bot met de naam W32.toxbot.b. In de beschrijving staat vermeld dat deze bot verbinding maakt met onder meer bovengenoemde domeinen (bijlage 9 van bijlage A001).
f. In een chatsessie van 29 maart 2005 met [getuige 1] verwijst [verdachte] naar betreffende beschrijving van Symantec van W32.toxbot.b en zegt (onder meer): "stomme av's, 'toxbot', had er duidelijk '[...]' op geplakt." (Het hof: zie in dit verband ook onder k).
g. [verdachte] verklaart in deze chatsessie verder dat hij sinds 2001 beschikt over bots, dat hij in de door hem gemaakte bot de toetsaanslagen op de binnengedrongen computers vastlegt en dat hij in 2003 heeft ontdekt hoeveel geld je ermee kunt verdienen.
h. Op basis van bovenstaande informatie werd een opsporingsonderzoek opgestart naar vermeende computervredebreuk.
(Proces-verbaal B1:)
i. Op grond van het onderzoek bleek verdachte samen met medeverdachte [medeverdachte] een botnetwerk

te beheren. In het internetverkeer was zichtbaar dat verdachte een virus dat hij beheerde en mogelijk muteerde regelmatig verstuurde naar [medeverdachte].
Zichtbaar was dat beiden commando's gaven aan het botnetwerk dat zij beheerden om nieuwe versies van het virus te verspreiden.
j. Tevens was zichtbaar dat de servers van het botnetwerk informatie gaven over de omvang van het botnetwerk. Zo was op 11 juli 2005 zichtbaar dat het botnetwerk uit meer dan 30.000 systemen bestond en op 8 augustus 2005 uit 50.095 systemen (bijlage 3 van proces-verbaal B1).
(Proces-verbaal B1.1:)
k. In een chat van 18 juli 2005 zegt verdachte dat hij eindelijk respect heeft en verwijst hij naar een website waarbij iemand refereert aan een virus met de naam Win32. [verdachte] en zegt hij dat de anderen het 'codbot' noemen en Symantec 'toxbot' (bijlage 1 van proces-verbaal B1.1).
l. In een testopstelling werd deze bot getest en werden de functionaliteiten beschreven. In een aanvullend proces-verbaal van 17 juli 2008 van verbalisanten [verbalisant 1] en [verbalisant 2] wordt een nadere omschrijving gegeven van de computers die zijn gebruikt in deze testopstelling (Het hof: zie hierna).
(Aanvullend proces-verbaal 17 juli 2008:)
m. In de testopstelling werden computers gebruikt die waren voorzien van het besturingssysteem Windows XP. Gebruikers van Windows XP kunnen er voor kiezen om dit systeem automatisch te laten voorzien van updates. Periodiek worden deze updates cumulatief aangeboden, zodat gebruikers ook in één keer alle updates kunnen installeren. Deze cumulatieve updates worden ook wel servicepacks genoemd. Ten tijde van het onderhavige onderzoek waren er reeds twee servicepacks, te weten Service Pack 1 (september 2002) en Service Pack 2 (augustus 2004). Het infecteren door de Toxbot blijkt te geschieden door het doorbreken van een beveiliging in Windows (XP) systemen die niet zijn voorzien van servicepack 2. Deze vorm van infectie is nagebootst in de testopstelling.
n. Door middel van deze infectiemethode kan het Toxbot virus een systeem binnendringen en zich daar nestelen als een programma. Om zich op deze manier als programma in een systeem als Windows te nestelen zijn 'administrator' of 'SYSTEM' rechten vereist op de betreffende computer.
o. Een standaard Windows XP installatie is beveiligd tegen het inloggen van buitenaf om daar vervolgens door middel van het gebruik van SYSTEM en/of administrator rechten programma's op te installeren.
(rapportage [verbalisant 1] 26 augustus 2008:)
p. Het Windows XP systeem is voorzien van talloze beveiligingen om onbevoegden van het systeem te weren. Het ontwikkelen van de updates en periodieke servicepacks is een reactie op de manieren die ontwikkeld zijn door hackers om deze beveiligingen te doorbreken of te omzeilen.
q. Uitgaande van het gegeven dat Windows XP standaard is voorzien van beveiliging is er voor gekozen om in de testopstelling gebruik te maken van XP systemen die niet zijn voorzien van updates of servicepacks. Temeer ook, omdat virussen als Toxbot zich juist richten op deze PC's.
r. In 2003 werden manieren ontdekt om via ingangen van hidden shares een beveiliging te doorbreken. Door middel van het opzettelijk geven van verkeerde signalen aan delen van het Windows besturingssysteem van PC's kan een systeem dusdanig in de war raken dat delen tijdelijk onbruikbaar raken of zelfs crashen. Dit is ook waargenomen bij de werking van het Toxbotvirus.
s. Om te voorkomen dat een (Toxbot)virus direct wordt gedetecteerd door een virusscanner wordt door hackers een techniek genaamd packing gebruikt. Deze techniek zorgt ervoor dat het virus wordt 'ingepakt' in een gecomprimeerd en versleuteld be-stand, waardoor het ondetecteerbaar blijft voor virusscanners.
(Proces-verbaal BI.2:)
t. Op 2 augustus 2005 wordt via afgetapte internetdata bij verdachte waargenomen dat op 28 juli 2005 een update commando werd gegeven door [verdachte] aan het botnetwerk. Dit commando hield in dat de geïnfecteerde computers in het botnetwerk de opdracht krijgen om ergens op het internet een nieuwe bot, genaamd tox.exe te downloaden en starten.
u. Het bestand tox.exe is door verbalisant [verbalisant 1] uitgevoerd op een computer met het Windows besturingssysteem. Het programma tox.exe bleek een nieuw uitvoerbaar programma met de naam mapi32.exe aan te maken. Het bestand bleek te zijn ver-sleuteld en gecomprimeerd (ofwel gepackt) zoals in de rapportage van 26 augustus 2008 is omschreven, om herkenning door virusscanners te voorkomen.
v. Na het scannen van dit bestand met een antivirusprogramma werd de bot geïdentificeerd als de W32.Toxbot.
D3.
Bij de beoordeling van dit ten laste gelegde feit is de juiste uitleg van de woorden "wederrechtelijk binnendringen" van belang. Het hof heeft daartoe gezocht naar de bedoeling van de wetgever. Van wederrechtelijk binnendringen in de zin van artikel 138a van het Wetboek van Strafrecht is sprake indien men zich de toegang verschaft tegen de onmiskenbare wil van de rechthebbende, welke zowel uit woorden als uit daden kan blijken.
Zoals uit de wetsgeschiedenis blijkt kan daarbij worden gedacht aan het plaatsen van een tekst op het beeldscherm dat toegang voor onbevoegden verboden is. Maar omdat deze woorden een per ongeluk tot stand gekomen toegang niet uitsluiten, bevat voornoemd artikel 138a onder meer ook het aanvullende vereiste dat sprake moet zijn van enige beveiliging, ofwel een kenbare drempel zodat onbevoegden zich niet simpelweg de toegang kunnen verschaffen. (Tweede Kamer, vergaderjaar 1991-1992, 21 551, nr. 11, pagina 18). Artikel 138a verlangt niet meer dan een minimale, doch wel daadwerkelijke beveiliging. Met andere woorden; indien het slachtoffer van computervredebreuk kan aantonen dat er sprake is van enige reële beveiliging dan is dat voldoende. (Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pagina 16).
D4.
Het hof leidt uit de vorenstaande onder Dl. ad m. tot en met q. opgenomen feiten en omstandigheden af dat iedere versie van Windows XP, zodra een particulier die aankoopt, is uitgerust met (een standaard) beveiliging. Naar het oordeel van het hof is hierbij sprake van enige reële beveiliging zoals hiervoor onder D3. is beschreven. Met betrekking tot deze beveiliging acht het hof tevens de rapportage van verbalisant

[verbalisant 1] van 26 augustus 2008 van belang, waar deze het volgende inhoudt:
"Als het gaat om een belangrijke beveiliging van XP in een netwerkomgeving als internet, is het volgende punt in dit verband het belangrijkste voorbeeld: Windows XP is een Windows variant uit de zogenaamde 'NT' familie, ontstaat uit Windows NT3.5 opgevolgd door Windows NT4.0, Windows 2000, Windows XP en Windows Vista. In de versies tot en met Windows 2000 was het in sommige gevallen mogelijk om deze via het netwerk te benaderen en er met gebruikmaking van Administratorrechten bestanden naar toe te sturen en zelfs uit te voeren. De genoemde methode maakte gebruik van de standaard door Windows aangemaakte verborgen shares als C$ en ADMIN$. Microsoft heeft deze optie van administrator toegang bij de introductie van XP bewust geblokkeerd en actief deze manier van niet-geautoriseerd gebruik beveiligd door deze toegang van buitenaf gebruik te laten maken van de geminimaliseerde rechten van het standaard aanwezige 'Guest' account. Een dergelijk Guest account heeft onvoldoende systeemrechten om die dingen te doen die door middel van het Toxbot virus wel worden gedaan. ( ) Het blokkeren van de verborgen shares nam voor anderen de laatste mogelijkheid weg om via het netwerk administrator rechten te verkrijgen zonder actief een beveiliging te doorbreken. In 2003 werden manieren ontdekt om via de oude ingangen van de hidden shares toch toegang te verkrijgen.".
Voorts blijkt uit hetgeen onder D1. ad r. tot en met u. is opgenomen dat verdachte het virus zodanig versleutelde en comprimeerde (het zogenoemde packing), dat het betreffende systeem het virus niet als een fout herkende. Het virus verspreidde zichzelf ver-volgens als een 'worm' middels de besmette computer naar andere computers. Deze werkwijze houdt naar het oordeel van het hof niets anders in dan dat verdachte niet alleen gaten in systeembeveiliging opzocht ten einde als administrator/system en aldus onder een valse hoedanigheid in de zin van artikel 138a van het Wetboek van Strafrecht, binnen te dringen, maar zich daarbij tevens bediende van een technische ingreep met behulp van valse signalen, te weten door in dit geval verhuld en onherkenbaar, middels het 'verpakte' virus binnen te dringen.
Gelet op de gehanteerde werkwijze, als hiervoor weergegeven is het hof van oordeel dat er sprake is van het doorbreken van de systeembeveiliging en van het verwerven van toegang middels een technische ingreep (tegen de onmiskenbare wil van de recht-hebbende) als bedoeld in artikel 138a van het Wetboek van Strafrecht.
D5.
Gelet op het vorenstaande onder D4 overwogene waren ook de versies van vóór Windows XP (onder meer Windows NT 3.5, Windows NT 4.0 en Windows 2000) voorzien van een minimale (standaard) beveiliging. Het vorenstaande heeft derhalve ook te gelden voor zover is binnengedrongen in Windows systemen anders dan Windows XP.
Het hof verwerpt in zoverre het verweer."

2.3. Art. 138a, eerste en derde lid, Sr luidde in de periode waarop de tenlastelegging betrekking heeft, als volgt:
"1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij
a. daarbij enige beveiliging doorbreekt of
b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.
(...)
3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens
(...)
b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde."

2.4. Het Hof heeft geoordeeld dat elke consumentenversie van het computerbesturingssysteem Windows XP is voorzien van enige beveiliging in de zin van art. 138a, eerste lid aanhef en onder a, (oud) Sr. Dat oordeel geeft in het licht van hetgeen het Hof zoals hiervoor weergegeven heeft overwogen geen blijk van een onjuiste rechtsopvatting en is niet onbegrijpelijk. Hierop stuit het middel af voor zover dat opkomt tegen de verwerping van het verweer dat door de verdachte en zijn mededader geen beveiliging is doorbroken. Opmerking verdient daarbij dat onder het doorbreken van enige beveiliging, zoals bedoeld in art. 138a, eerste lid onder a, (oud) Sr, mede dient te worden verstaan het tegen de wil van de rechthebbende binnendringen in een computer langs een weg die de aanwezige beveiliging niet of onvoldoende afsluit. Daarbij is, anders dan de steller van het middel betoogt, niet van belang of die opening inherent is aan het systeem of is veroorzaakt door andere 'aanvallers'.

2.5. Voor zover het middel opkomt tegen de verwerping van het verweer dat geen sprake is van een technische ingreep met de klacht dat dit niet uit de bewijsmiddelen kan worden afgeleid, faalt het bij gebrek aan feitelijke grondslag. Het middel berust immers op een onjuiste lezing van 's Hofs arrest, waar het betoogt dat het Hof zou hebben geoordeeld dat de technische ingreep enkel zou bestaan in het verpakken van het virus. Het oordeel van het Hof moet immers aldus worden verstaan dat het als de in de bewezenverklaring bedoelde technische ingreep heeft aangemerkt het samenstel van alle handelingen die nodig waren voor de verspreiding van het virus. Dat oordeel geeft geen blijk van een onjuiste rechtsopvatting en is niet onbegrijpelijk.

2.6. Het middel faalt.

3. Beoordeling van het middel van de Advocaat-Generaal bij het Hof

3.1. Het middel behelst de klacht dat het Hof bij de gegeven vrijspraak van het aan de verdachte onder 2 en 3 tenlastegelegde een onjuiste uitleg heeft gegeven aan art. 161sexies, aanhef en onder 2°, (oud) Sr, in het bijzonder aan de aan die bepaling ontleende en in de tenlastelegging opgenomen bestanddelen "geautomatiseerd werk" en "gemeen gevaar voor de verlening van diensten".

3.2.1. Aan de verdachte is onder 2 en 3 tenlastegelegd dat:
"2.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 6 juli 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk één of meer geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten één of meer computer(s) en/of server(s), heeft beschadigd of onbruikbaar gemaakt en/of stoornis in de gang of in de werking van zodanig werk heeft veroorzaakt en/of een ten opzichte van zodanig werk genomen veiligheidsmaatregelen heeft verijdeld,
immers, heeft/hebben verdachte en/of zijn mededader(s) (telkens)
- één of meer (versie(s) van een) virus(en) en/of trojan(s) gemaakt en/of ontwikkeld ((onder meer) bekend onder de naam Wayphisher) en/of;
- (aan een/zijn botnetwerk) één of meer opdracht(en) gegeven het/de (door verdachte en/of zijn mededader(s) (mede) gemaakte en/of ontwikkelde (versie(s) virus(sen) en/of trojan(s) te downloaden en/of op de betreffende en/of één of meer andere computer(s) te installeren (waarna het betreffende virus en/of trojan is geïnstalleerd) waardoor gemeen gevaar voor goederen en/of voor de verlening van diensten te duchten is geweest immers,
- de gebruikers van de aldus 'besmette' computer(s) waren niet meer in staat om betrouwbaar gebruik te maken van een/de online (bancaire) dienst(en) (die doelwit waren van het virus en/of de trojan) (immers werd die gebruiker bij/na het gebruik van (een) internetadressen) (van(een) bank(en)) omgeleid naar één of meer andere internetadressen en/of (waarna) de inloggegevens (ten behoeve van het online/electronisch bankieren) konden en/of werden onderschept) en/of
- (waarna) verdachte en/of zijn mededader(s) de beschikking kre(e)g(en) over bancaire en/of andere gegeven(s) toebehorende aan één of meer van die gebruiker(s);
3.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 6 juli 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk één of meer geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten één of meer computer(s) en/of server(s), heeft beschadigd of onbruikbaar gemaakt en/of stoornis in de gang of in de werking van zodanig werk heeft veroorzaakt en/of een ten opzichte van zodanig werk genomen veiligheidsmaatregelen heeft verijdeld,
immers, heeft/hebben verdachte en/of zijn mededader(s) (telkens):
- één of meer (versie(s) van een) virus(sen) gemaakt en/of ontwikkeld ((onder meer) bekend onder de naam Toxbot) en/of
- dit/deze virus(sen) op één of meer andere computer(s) geïnstalleerd en/of doen installeren,
waarna het/de (aldus besmette) geautomatiseerde werk(en) (vervolgens) (automatisch) herstartte(n) en/of crashte(n), waardoor gemeen gevaar voor goederen en/of voor de verlening van diensten te duchten is geweest,
immers werden (hierdoor) de toetsaanslagen van de gebruiker(s) van de aldus besmette computer(s) (zonder medeweten van die gebruiker(s)) vastgelegd, waardoor verdachte en/of zijn mededader(s) de beschikking kre(e)g(en) over:
- financiële/bancaire gegevens van één of meer bank(en) en/of creditcard maatschappijen) en/of;
- inlog- en wachtwoordgegevens van één of meer Paypal-account(s) en/of;
- inlog- en wachtwoordgegevens van één of meer Ebay-account(s) en/of;
- één of meer ander(e) gegeven(s)
van (één of meer van) die gebruiker(s)."

3.2.2. Het Hof heeft de verdachte van het onder 2 en 3 tenlastegelegde vrijgesproken. Het heeft dienaangaande overwogen:
"Op grond van het onderzoek ter terechtzitting in hoger beroep is het volgende gebleken. Aan verdachte is onder 2 en 3 telkens ten laste gelegd het misdrijf als bedoeld in artikel 161sexies, aanhef en onder 2°, van het Wetboek van Strafrecht, zoals dit artikel luidde in de ten laste gelegde periode, en waarin is strafbaar gesteld:
"hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is".
Bij de beoordeling van deze ten laste gelegde feiten is de juiste uitleg van de woorden "gemeen gevaar voor goederen of voor de verlening van diensten" van belang. Het hof heeft daartoe gezocht naar de bedoeling van de wetgever.
De wetgever heeft artikel 161sexies een plaats gegeven in Titel VII van het Tweede Boek van het Wetboek van Strafrecht, waarin "Misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht" worden omschreven.
Voorts blijkt uit de Memorie van Toelichting dat deze bepaling ziet op gedragingen die gevaar veroorzaken voor personen of goederen, zonder dat deze gedragingen zich richten tegen bepaalde goederen of bepaalde personen (Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pagina 19).

Ook in de Memorie van Antwoord geeft de minister aan dat het voorgestelde artikel betrekking heeft op een dienst met "gegevensverwerking of telecommunicatie ten algemene nutte" (Tweede Kamer, vergaderjaar 1989-1990, 21551, nr. 6, pagina 36).
De wetgever heeft kennelijk de strafrechtelijke bescherming van geautomatiseerde werken die gemeen/ ten algemene nutte worden gebruikt, voor ogen gehad.
Het hof is van oordeel dat op grond van de wettige bewijsmiddelen niet is komen vast te staan dat als gevolg van de handelingen van verdachte gemeen gevaar voor goederen of voor de verlening van diensten te duchten is geweest. Het hof kan (slechts) vaststellen dat verdachte via de besmetting met een virus een storing heeft veroorzaakt in de computers van individuele gebruikers (zijnde de computers van de particulieren en/of de bedrijven welke deel uitmaakten van het botnetwerk van verdachte). Deze (rechtspersonen waren daardoor (tijdelijk) niet in staat op een veilige wijze gebruik te maken van geautomatiseerde werken van bancaire instellingen of creditcardmaatschappijen.
Niet is komen vast te staan dat ook een storing is veroorzaakt in geautomatiseerde werken van de betreffende bancaire instellingen of creditcardmaatschappijen zelf, waardoor er een gemeen gevaar zou kunnen zijn ontstaan voor de verlening van diensten aan de vele (andere) gebruikers van deze geautomatiseerde werken.
Het hof is op grond van het vorenstaande van oordeel, dat het onder 2 en 3 ten laste gelegde niet kan worden bewezen verklaard."

3.3. Het middel stelt in het bijzonder de vraag aan de orde of gemeen gevaar voor de verlening van diensten kan zijn te duchten in de zin van art. 161sexies, aanhef en onder 2°, (oud) Sr, indien het handelen van de verdachte niet is gericht op de computers van dienstverlenende instellingen, maar op de computers van afnemers van de desbetreffende diensten.

3.4.1. Art. 161sexies, aanhef en onder 2°, Sr luidde in de periode waarop de tenlastelegging betrekking heeft als volgt:
"Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:
(...)
2°. met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is."

3.4.2. Aan de totstandkomingsgeschiedenis van de Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit), Stb. 1993, 33, waarbij art. 161sexies Sr is ingevoerd, kan het volgende worden ontleend waar het betreft de memorie van toelichting:
"In het algemeen is getracht in de juridische omschrijvingen zoveel mogelijk te abstraheren van de huidige stand der techniek en in de plaats daarvan aansluiting te zoeken bij de maatschappelijke functie van de nieuwe technische mogelijkheden. Dit betekent dat gezocht is naar begrippen die ook bruikbaar blijven indien door nieuwe technische ontwikkelingen op geheel andere wijze dan thans toch dezelfde maatschappelijke functie op informatietechnologisch gebied wordt vervuld.
(...)
Een tweede nieuw begrip dat in dit wetsvoorstel wordt geïntroduceerd is dat van een "geautomatiseerd werk". Hieronder wordt verstaan elke inrichting die met technische middelen geschikt is gemaakt voor de opslag, verwerking of overdracht van gegevens. Het begrip "geautomatiseerd" duidt op een functioneren van het werk voor een deel onafhankelijk van menselijk ingrijpen. Hieronder vallen dus computers, netwerken van aan elkaar verbonden computers en inrichtingen voor telecommunicatie. Hieronder vallen dus niet werken die uitsluitend bestemd zijn voor de opslag van gegevens of eenvoudige werken die in beginsel slechts bestemd zijn om te functioneren zonder interactie met hun omgeving, zoals een elektronisch klokje.
(...)
Titel VII van het Tweede Boek van het Wetboek van Strafrecht draagt het opschrift "Misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht". De titel bevat bepalingen die zien op gedragingen die gevaar veroorzaken voor personen of goederen, zonder dat deze gedragingen zich richten tegen bepaalde goederen of personen. Het gaat bij voorbeeld om brandstichting, aantasting van de elektriciteitsvoorziening, het blootstellen aan radioactiviteit, de verstoring van het weg-, scheepvaart- of luchtverkeer en ernstige verontreinigingen van het milieu. De afhankelijkheid van de tegenwoordige samenleving van de geautomatiseerde opslag, verwerking en overdracht van gegevens is zo groot dat een daarop betrekking hebbende bepaling in deze Titel wenselijk is.
De voorgestelde bepaling sluit aan bij de bestaande bepalingen in deze Titel. In wezen gaat het er om dat steeds, zo niet dezelfde, dan toch in zwaarte vergelijkbare belangen worden gediend. De verschillende bepalingen onderscheiden zich naar de herkomst van de bedreiging van deze belangen. De plaats die de geautomatiseerde opslag, verwerking en overdracht van gegevens in de samenleving is gaan innemen, rechtvaardigt de strafbaarstelling van een mogelijke aantasting van deze belangen vanuit deze optiek.
Op overeenkomstige wijze als de andere bepalingen in deze titel zijn opgezet, is onderscheiden tussen een opzet- en een schuldvariant. De schuld omvat volgens vaste jurisprudentie niet alle, ook de geringste onachtzaamheid, maar alleen een min of meer grove of aanmerkelijke onvoorzichtigheid, onachtzaamheid of nalatigheid.
Nieuw is dat onder de te beschermen belangen ook de verlening van diensten is opgenomen. De verlening van diensten is in economisch opzicht in de informatiemaatschappij van vergelijkbaar belang als de produktie van en de handel in goederen. Overigens gaat het in dit artikel niet alleen om de commerciële

dienstverlening, doch ook om de non-commerciële, bij voorbeeld in de sfeer van de gezondheidszorg." (Kamerstukken II 1989-1990, 21 551, nr. 3, p. 4-6 en p. 19-20)

waar het betreft de memorie van antwoord:
"Het "gemeen" gevaar ziet, zoals ook blijkt uit het opschrift van Titel VII, waarin de voorgestelde bepaling zal worden ingevoegd, op de algemene veiligheid.
Noyon-Langemeijer-Remmelink zegt hierover dat de veroorzaker van het gevaar de omvang van het gevaar vooraf niet kan berekenen of naar willekeur bepalen. Gemeen gevaar voor de verlening van diensten ziet dus op een zodanige stoornis van een geautomatiseerd werk dat vooraf geen inzicht kan worden gevormd over de omvang van de schade die daardoor wordt aangericht. Beperkt de stoornis zich tot een computer die betrekking heeft op een bepaald soort dienstverlening, die door de schade uitvalt, zonder dat verderstrekkende gevolgen kunnen intreden, dan is er geen sprake van gemeen gevaar. Bij dit alles is het van geen belang of de dienstverlening plaatsvindt ten algemenen nutte dan wel binnen een sector van het bedrijfsleven, bij voorbeeld het bankwezen.
De verhindering en bemoeilijking van de opslag of verwerking van gegevens is van een geheel andere orde. Geenszins behoeft daardoor de dienstverlening in gevaar te komen. Evenmin gaat het om een gevaar. Slechts indien daadwerkelijk de opslag of verwerking wordt belemmerd, is er sprake van strafbaarheid. Te denken valt aan een merkbare vertraging in het functioneren van een geautomatiseerd werk of in hinderlijke fouten in het functioneren van de computer die steeds moeten worden hersteld. De reikwijdte van deze strafbepaling is beperkt tot geautomatiseerde werken ten algemenen nutte. Dan is er immers een belang van ruimere strekking dan alleen het belang van de desbetreffende organisatie. Binnen het particuliere bedrijfsleven is men aangewezen op civielrechtelijke middelen, bij voorbeeld het ontslag van het personeel dat de bemoeilijking veroorzaakt. Voor alle duidelijkheid wijs ik erop dat het hier niet gaat om een storing die wordt veroorzaakt doordat programmagegevens worden gewijzigd. Is dit het geval dan wordt het voorgestelde artikel 350a overtreden."
(Kamerstukken II 1990-1991, 21551, nr. 6, p. 13).

3.5. In de tekst van art. 161sexies, aanhef en onder 2°, (oud) Sr wordt wat betreft de term "geautomatiseerd werk" geen onderscheid gemaakt tussen computers van dienstverlenende instellingen en computers van afnemers van diensten.
Ook in de wetsgeschiedenis wordt dat onderscheid niet gemaakt. Blijkens de hiervoor weergegeven onderdelen van die wetsgeschiedenis beoogde de wetgever met de invoering van deze bepaling onder meer strafrechtelijke bescherming te verlenen aan het belang van de verlening van diensten, voor zover deze in gevaar gebracht kan worden door, onder meer, het opzettelijk veroorzaken van een stoornis in de werking van een geautomatiseerd werk.
Onder het begrip geautomatiseerd werk dienen, aldus de memorie van toelichting, ook computers en netwerken van aan elkaar verbonden computers te worden begrepen, terwijl in het verlengde daarvan op grond van de door de wetgever voorgestane dynamische wetsuitleg daarbij tegenwoordig ook moet worden gedacht aan, zoals in het onderhavige geval, een reeks van computers die door middel van schadelijke, via het internet verspreide software met elkaar zijn verbonden.
Onder "gemeen gevaar" dient in dit verband mede te worden verstaan het gevaar voor een ongestoorde dienstverlening aan een onbestemd doch aanmerkelijk aantal afnemers.
Uit een en ander moet worden afgeleid dat voor de beantwoording van de vraag of een stoornis is veroorzaakt in een geautomatiseerd werk en of daarvan gemeen gevaar voor de verlening van diensten te duchten is geweest, zoals bedoeld in art. 161sexies, aanhef en onder 2°, (oud) Sr, niet van doorslaggevende betekenis is of die stoornis wordt veroorzaakt in de computers van de afnemers van een dienst, ook als die door een netwerk aan elkaar zijn verbonden, dan wel van dergelijke computers van de dienstverlener, maar dat het erom gaat of van de opzettelijk veroorzaakte stoornis gemeen gevaar te duchten was voor een ongestoorde dienstverlening.

3.6. Het Hof heeft geoordeeld dat de wetgever met de strafbaarstelling van art. 161sexies, aanhef en onder 2°, Sr "kennelijk de strafrechtelijke bescherming van geautomatiseerde werken die gemeen/ten algemene nutte worden gebruikt, voor ogen [heeft] gehad" en heeft aan het bewijs van het te duchten gemeen gevaar voor de verlening van diensten de voorwaarde verbonden dat "een storing is veroorzaakt in geautomatiseerde werken van de betreffende bancaire instellingen of creditcardmaatschappijen zelf".
Het Hof heeft daarbij kennelijk onderscheid gemaakt tussen de computers van de afnemers van een dienst en de computers van de dienstverlener, in die zin dat een stoornis in de computers van de afnemers niet het in de meergenoemde bepaling bedoelde te duchten gemeen gevaar voor de verlening van diensten kan opleveren.
Daarmee heeft het Hof miskend hetgeen hiervoor onder 3.5 is overwogen en heeft het aan de vrijspraak van de verdachte van de onder 2 en 3 tenlastegelegde feiten een onjuiste rechtsopvatting ten grondslag gelegd.

3.7. Het middel is dus terecht voorgesteld.

4. Slotsom

Nu de Hoge Raad geen grond aanwezig oordeelt waarop de bestreden uitspraak ambtshalve zou behoren te worden vernietigd, brengt hetgeen hiervoor is overwogen mee dat als volgt moet worden beslist.

5. Beslissing

De Hoge Raad:

vernietigt de bestreden uitspraak maar uitsluitend wat betreft de beslissingen ter zake van het onder 2 en 3 tenlastegelegde en de strafoplegging;
verwijst de zaak naar het Gerechtshof te 's-Gravenhage, opdat de zaak in zoverre op het bestaande hoger beroep opnieuw wordt berecht en afgedaan;
verwerpt het beroep voor het overige.

Dit arrest is gewezen door de vice-president A.J.A. van Dorst als voorzitter, en de raadsheren B.C. de Savornin Lohman, J.W. Ilsink, J. de Hullu en M.A. Loth, in bijzijn van de griffier S.P. Bakker, en uitgesproken op 22 februari 2011.

Conclusie
Nr. 09/02184
Mr. Knigge
Zitting: 28 september 2010

Conclusie inzake:

[Verdachte]

1. Verdachte is door het Gerechtshof te 's-Hertogenbosch wegens 1. "medeplegen van computervredebreuk meermalen gepleegd", 6. "poging tot afpersing, terwijl het feit wordt gepleegd door twee of meer verenigde personen", 7. "medeplegen van oplichting, meermalen gepleegd" en 9. "handelen in strijd met artikel 13, eerste lid van de Wet wapens en munitie" veroordeeld tot een gevangenisstraf voor de duur van 730 dagen, waarvan 405 dagen voorwaardelijk met een proeftijd van 2 jaren, met de beslissingen ten aanzien van inbeslaggenomen voorwerpen als weergegeven in het arrest.

2. De beroepen zijn ingesteld door de Advocaat-Generaal bij het Hof en namens de verdachte. De plaatsvervangend Advocaat-Generaal bij het Hof heeft bij schriftuur een middel van cassatie voorgesteld, gericht tegen de vrijspraken ter zake van de onder 2 en 3 tenlastegelegde feiten. Namens de verdachte heeft mr. S.B.J. Hiemstra, advocaat te Haarlem, bij schriftuur een middel van cassatie voorgesteld, gericht tegen de bewezenverklaring van het onder 1 tenlastegelegde feit.

Algemeen
3. Het gaat in deze zaak om het volgende. De verdachte en zijn medeverdachte hebben een groot aantal computers geïnfecteerd met verschillende versies van een door de verdachte zelf ontwikkeld virus, het W32.Toxbot-virus. Door middel van dit Toxbot-virus werd een botnet(werk) tot stand gebracht.(1) De verdachten hadden aldus, als beheerders van het netwerk, de controle over de geïnfecteerde computers. Het Toxbotvirus was voorzien van verschillende "functionaliteiten", die door middel van opdrachten door de verdachten konden worden geactiveerd.(2) Zo konden de verdachten het virus de opdracht geven zich over andere, nog niet geïnfecteerde computers te verspreiden.(3) Het botnet breidde zich daardoor uit. Zo omvatte het netwerk op 11 juli 2005 meer dan 30.000 geïnfecteerde computers, terwijl het op 8 augustus 2005 al uit 50.096 computers bestond.(4) Op dit infecteren van computers ziet het onder 1 tenlastegelegde (computervredebreuk).
Tot de opdrachten die aan de bots gegeven konden worden, behoorde ook de opdracht een bepaalde trojan (Wayphisher) te downloaden en te installeren.(5) Deze trojan zorgde ervoor dat nietsvermoedende internetbankierende computergebruikers werden omgeleid naar een ander internetadres en zo hun financiële gegevens (gebruikersnamen, wachtwoorden, enz.) invulden op inlogschermen die bedrieglijk veel op die van de bank leken. Ook op andere wijze werden inloggegevens onderschept. Tot de functionaliteiten van het Toxbotvirus behoorde het vastleggen en versturen van toetsenbordaanslagen door zogenaamde keyloggers. Deze functionaliteit werd geactiveerd zodra de gebruiker een internetadres intypte waarin bepaalde woorden (zoals bank, login, ebay en paypal) voorkwamen. Op dit doen installeren van het Wayphister-trojan en van de (van het Toxbotvirus deeluitmakende) keyloggers zien de onder 2 en 3 tenlastegelegde feiten (art. 161sexies Sr).(6)
De aldus onderschepte inloggegevens werden door de verdachten gebruikt voor het doen van bestellingen op internet ten koste van de rekeninghouders. De verdachten werkten voorts aan een methode om met behulp van de onderschepte gegevens geld van privérekeningen over te maken naar eigen rekeningen.

4. Voor zover voor de beoordeling van de middelen relevant, is aan de verdachte tenlastegelegd dat:
"1.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 1 juni 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk wederrechtelijk in een geautomatiseerd werk voor de opslag of verwerking van gegevens, te weten één of meer computers) en/of server(s), of in een deel daarvan, is binnengedrongen, waarbij hij, verdachte en/of zijn medeverdachte(n) de beveiliging heeft/hebben doorbroken, in elk geval de toegang heeft/hebben verworven door een technische ingreep, met behulp van valse signalen en/of een valse sleutel en/of door het aannemen van een valse hoedanigheid, namelijk (telkens) door (, gebruikmakend van één of meer kwetsbaarhe(i)d(en) in het besturingssysteem van Windows,) een (al dan niet door verdachte en/of één van zijn mededader(s) gemaakt(e)/ontwikkeld(e)) (versie van een) virus, (onder meer) bekend onder de naam Toxbot, te (doen) verspreiden en/of te (doen) installeren waarna hij, verdachte en/of zijn mededader(s), door tussenkomst van het geautomatiseerde werk waarin hij/zij is/zijn binnengedrongen de

toegang heeft/hebben verworven tot één of meer geautomatiseerde werk(en) van één of meer derde(n);

2.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 6 juli 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk één of meer geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten één of meer computer(s) en/of server(s), heeft beschadigd of onbruikbaar gemaakt en/of stoornis in de gang of in de werking van zodanig werk heeft veroorzaakt en/of een ten opzichte van zodanig werk genomen veiligheidsmaatregelen heeft verijdeld,
immers, heeft/hebben verdachte en/of zijn mededader(s) (telkens)
- één of meer (versie(s) van een) virus(en) en/of trojan(s) gemaakt en/of ontwikkeld ((onder meer) bekend onder de naam Wayphisher) en/of;
- (aan een/zijn botnetwerk) één of meer opdracht(en) gegeven het/de (door verdachte en/of zijn mededader(s) (mede) gemaakte en/of ontwikkelde (versie(s) virus(sen) en/of trojan(s) te downloaden en/of op de betreffende en/of één of meer andere computer(s) te installeren (waarna het betreffende virus en/of trojan is geïnstalleerd) waardoor gemeen gevaar voor goederen en/of voor de verlening van diensten te duchten is geweest
immers,
- de gebruikers van de aldus 'besmette' computer(s) waren niet meer in staat om betrouwbaar gebruik te maken van een/de online (bancaire) dienst(en) (die doelwit waren van het virus en/of de trojan) (immers werd die gebruiker bij/na het gebruik van (een) internetadressen) (van(een) bank(en)) omgeleid naar één of meer andere internetadressen en/of (waarna) de inloggegevens (ten behoeve van het online/electronisch bankieren) konden en/of werden onderschept)
en/of
- (waarna) verdachte en/of zijn mededader(s) de beschikking kre(e)g(en) over bancaire en/of andere gegeven(s) toebehorende aan één of meer van die gebruiker(s);

3.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 6 juli 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk één of meer geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten één of meer computer(s) en/of server(s), heeft beschadigd of onbruikbaar gemaakt en/of stoornis in de gang of in de werking van zodanig werk heeft veroorzaakt en/of een ten opzichte van zodanig werk genomen veiligheidsmaatregelen heeft verijdeld,
immers, heeft/hebben verdachte en/of zijn mededader(s) (telkens):
- één of meer (versie(s) van een) virus(sen) gemaakt en/of ontwikkeld ((onder meer) bekend onder de naam Toxbot) en/of
- dit/deze virus(sen) op één of meer andere computer(s) geïnstalleerd en/of doen installeren,
waarna het/de (aldus besmette) geautomatiseerde werk(en) (vervolgens) (automatisch) herstartte(n) en/of crashte(n), waardoor gemeen gevaar voor goederen en/of voor de verlening van diensten te duchten is geweest,
immers werden (hierdoor) de toetsaanslagen van de gebruiker(s) van de aldus besmette computer(s) (zonder medeweten van die gebruiker(s)) vastgelegd, waardoor verdachte en/of zijn mededader(s) de beschikking kre(e)g(en) over:
- financiële/bancaire gegevens van één of meer bank(en) en/of creditcard maatschappijen) en/of;
- inlog- en wachtwoordgegevens van één of meer Paypal-account(s) en/of;
- inlog- en wachtwoordgegevens van één of meer Ebay-account(s) en/of;
- één of meer ander(e) gegeven(s)
van (één of meer van) die gebruiker(s)".

5. Van het onder 2 en 3 tenlastegelegde heeft het Hof vrijgesproken. Onder 1 heeft het Hof bewezenverklaard dat:
"1.
Hij op tijdstippen in de periode van 1 juni 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met een ander, telkens opzettelijk wederrechtelijk in een geautomatiseerd werk voor de opslag of verwerking van gegevens, te weten computers, is binnengedrongen, waarbij hij, verdachte en zijn medeverdachte de beveiliging hebben doorbroken, in elk geval de toegang hebben verworven door een technische ingreep, met behulp van valse signalen en/of door het aannemen van een valse hoedanigheid, namelijk telkens door, gebruikmakend van één of meer kwetsbaarheden in het besturingssysteem van Windows, een (al dan niet door verdachte gemaakte/ontwikkelde) versie van een virus, onder meer bekend onder de naam Toxbot, te (doen) verspreiden en/of te (doen) installeren waarna hij, verdachte en zijn mededader, door tussenkomst van het geautomatiseerde werk waarin zij zijn binnengedrongen de toegang hebben verworven tot geautomatiseerde werken van derden".

6. De artikelen 138a en 161sexies Sr luidden in tenlastegelegde periode:
"138a
1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij
a. daarbij enige beveiliging doorbreekt of
b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel 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 in een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt.
3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens
a. met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;
b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde."

"161sexies
Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:
1°. met gevangenisstraf van ten hoogste zes maanden of geldboete van de vijfde categorie, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, ontstaat;
2°. met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is."

7. Van belang zijn ook de artikelen 326c en 350a Sr. Die luidden in de tenlastegelegde periode:
"326c
1. Hij die, met het oogmerk daarvoor niet volledig te betalen, door een technische ingreep of met behulp van valse signalen, gebruik maakt van een dienst die via telecommunicatie aan het publiek wordt aangeboden, wordt gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vijfde categorie.
2. Met gevangenisstraf van een jaar of geldboete van de derde categorie wordt gestraft hij die opzettelijk een voorwerp dat kennelijk is bestemd, of gegevens die kennelijk zijn bestemd, tot het plegen van het misdrijf, bedoeld in het eerste lid,
a. openlijk ter verspreiding aanbiedt;
b. ter verspreiding of met het oog op de invoer in Nederland voorhanden heeft of
c. uit winstbejag vervaardigt of bewaart.
3. Hij die van het plegen van misdrijven als bedoeld in het tweede lid, zijn beroep maakt of het plegen van deze misdrijven als bedrijf uitoefent wordt gestraft hetzij met gevangenisstraf van ten hoogste drie jaren en geldboete van de vijfde categorie, hetzij met één van deze straffen."

"350a
1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.
2. Hij die het feit, bedoeld in het eerste lid, pleegt na door tussenkomst van een openbaar telecommunicatienetwerk, wederrechtelijk in een geautomatiseerd werk te zijn binnengedrongen en daar ernstige schade met betrekking tot die gegevens veroorzaakt, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.
3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
4. Niet strafbaar is degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken."

8. Het op 1 september 2006 ingevoerde art. 138b Sr(7) luidt:
"138b
Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden."

9. In het navolgende zal ik eerst het middel van de plaatsvervangend Advocaat-Generaal bespreken; het middel van de verdachte komt daarna aan de orde.

Het middel van de plaatsvervangend Advocaat-Generaal
10. Het middel klaagt dat het Hof de grondslag van de tenlastelegging heeft verlaten, nu het de verdachte van het onder 2 en 3 tenlastegelegde heeft vrijgesproken, en daarbij een onjuiste uitleg heeft gegeven aan de in die tenlastelegging voorkomende begrippen "geautomatiseerd werk" en/of "gemeen gevaar voor de verlening van diensten".

11. Voor zover voor de beoordeling van het middel relevant, houdt het bestreden arrest in:
"Ten aanzien van het onder 2 en 3 ten laste gelegde.
Op grond van het onderzoek ter terechtzitting in hoger beroep is het volgende gebleken.
Aan verdachte is onder 2 en 3 telkens ten laste gelegd het misdrijf als bedoeld in artikel 161sexies, aanhef en

onder 2°, van het Wetboek van Strafrecht, zoals dit artikel luidde in de ten laste gelegde periode, en waarin is strafbaar gesteld:

"hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is".

Bij de beoordeling van deze ten laste gelegde feiten is de juiste uitleg van de woorden "gemeen gevaar voor goederen of voor de verlening van diensten" van belang. Het hof heeft daartoe gezocht naar de bedoeling van de wetgever.

De wetgever heeft artikel 161sexies een plaats gegeven in Titel VII van het Tweede Boek van het Wetboek van Strafrecht, waarin "Misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht" worden omschreven.
Voorts blijkt uit de Memorie van Toelichting dat deze bepaling ziet op gedragingen die gevaar veroorzaken voor personen of goederen, zonder dat deze gedragingen zich richten tegen bepaalde goederen of bepaalde personen (Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pagina 19).
Ook in de Memorie van Antwoord geeft de minister aan dat het voorgestelde artikel betrekking heeft op een dienst met "gegevensverwerking of telecommunicatie ten algemene nutte"
(Tweede Kamer, vergaderjaar 1989-1990, 21551, nr. 6, pagina 36).
De wetgever heeft kennelijk de strafrechtelijke bescherming van geautomatiseerde werken die gemeen/ ten algemene nutte worden gebruikt, voor ogen gehad.

Het hof is van oordeel dat op grond van de wettige bewijsmiddelen niet is komen vast te staan dat als gevolg van de handelingen van verdachte gemeen gevaar voor goederen of voor de verlening van diensten te duchten is geweest. Het hof kan (slechts) vaststellen dat verdachte via de besmetting met een virus een storing heeft veroorzaakt in de computers van individuele gebruikers (zijnde de computers van de particulieren en/of de bedrijven welke deel uitmaakten van het botnetwerk van verdachte). Deze (rechtspersonen waren daardoor (tijdelijk) niet in staat op een veilige wijze gebruik te maken van geautomatiseerde werken van bancaire instellingen of creditcardmaatschappijen.
Niet is komen vast te staan dat ook een storing is veroorzaakt in geautomatiseerde werken van de betreffende bancaire instellingen of creditcardmaatschappijen zelf, waardoor er een gemeen gevaar zou kunnen zijn ontstaan voor de verlening van diensten aan de vele (andere) gebruikers van deze geautomatiseerde werken.

Het hof is op grond van het vorenstaande van oordeel, dat het onder 2 en 3 ten laste gelegde niet kan worden bewezen verklaard."

12. De vraag waarop het middel zich toespitst, is of het gemeen gevaar voor de verlening van diensten waarvan art. 161sexies Sr spreekt, te duchten moet zijn van de vernieling (enz.) van een geautomatiseerd werk dat bij de dienstverlener in gebruik is. Het Hof beantwoordt die vraag kennelijk bevestigend. De indiener van het middel daarentegen stelt zich op het standpunt dat ook de vernieling (enz.) van computers die bij de afnemers van de diensten in gebruik zijn het strafbare feit van art. 161sexies Sr oplevert als daarvan gemeen gevaar voor de verlening van diensten te duchten is. De vraag die daar doorheen speelt, is wat onder het bedoelde gemeen gevaar moet worden verstaan.

13. De Memorie van Toelichting op het wetsvoorstel strekkende onder meer tot invoering van artikel 161sexies Sr (Wet computercriminaliteit) houdt onder meer in:
"Titel VII van het Tweede Boek van het Wetboek van Strafrecht draagt het opschrift "Misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht". De titel bevat bepalingen die zien op gedragingen die gevaar veroorzaken voor personen of goederen, zonder dat deze gedragingen zich richten tegen bepaalde goederen of personen. Het gaat bij voorbeeld om brandstichting, aantasting van de elektriciteitsvoorziening, het blootstellen aan radioactiviteit, de verstoring van het weg-, scheepvaart- of luchtverkeer en ernstige verontreinigingen van het milieu. De afhankelijkheid van de tegenwoordige samenleving van de geautomatiseerde opslag, verwerking en overdracht van gegevens is zo groot dat een daarop betrekking hebbende bepaling in deze Titel wenselijk is.
De voorgestelde bepaling sluit aan bij de bestaande bepalingen in deze Titel. In wezen gaat het er om dat steeds, zo niet dezelfde, dan toch in zwaarte vergelijkbare belangen worden gediend. De verschillende bepalingen onderscheiden zich naar de herkomst van de bedreiging van deze belangen. De plaats die de geautomatiseerde opslag, verwerking en overdracht van gegevens in de samenleving is gaan innemen, rechtvaardigt de strafbaarstelling van een mogelijke aantasting van deze belangen vanuit deze optiek.
Op overeenkomstige wijze als de andere bepalingen in deze titel zijn opgezet, is onderscheiden tussen een opzet- en een schuldvariant. De schuld omvat volgens vaste jurisprudentie niet alle, ook de geringste onachtzaamheid, maar alleen een min of meer grove of aanmerkelijke onvoorzichtigheid, onachtzaamheid of nalatigheid.
Nieuw is dat onder de te beschermen belangen ook de verlening van diensten is opgenomen. De verlening van diensten is in economisch opzicht in de informatiemaatschappij van vergelijkbaar belang als de produktie van en de handel in goederen. Overigens gaat het in dit artikel niet alleen om de commerciële dienstverlening, doch ook om de non-commerciële, bij voorbeeld in de sfeer van de gezondheidszorg.
De vraag kan rijzen of deze bepalingen niet te ver reiken in die zin dat daarmee bij voorbeeld het personeel van de P.T.T. wordt verboden in geval van een staking de goede werking van de telecommunicatie-

infrastructuur te storen. De rechter zal immers niet licht aannemen dat in geval tijdens een staking met de voorgestelde bepaling de goede werking van de telecommunicatie-infrastructuur wordt gestoord, er sprake zal zijn van overmacht in de zin van artikel 40 van het Wetboek van Strafrecht. Zou men menen dat de eventuele gevolgen van een dergelijke staking buiten de sfeer van de strafrechtelijke aansprakelijkheid dienen te blijven, dan zou overwogen kunnen worden, in de zinsnede die betrekking heeft op de stoornis in de telecommunicatie-infrastructuur het bestanddeel "wederrechtelijk" op te nemen. De moderne samenleving is echter in toenemende mate afhankelijk van het ongestoord functioneren van voorzieningen als die van de telecommunicatie-infrastructuur. Daarnaast maken de ontwikkelingen in de techniek het steeds meer mogelijk ook met geringe inzet van personeel toch de telecommunicatie-infrastructuur te laten blijven functioneren. In het licht van het bovenstaande acht ik het gerechtvaardigd de strafbaarstelling van de artikelen 161 bis en 161 ter ongewijzigd te laten en de voorgestelde artikelen 161sexies en 161septies op dezelfde leest te schoeien. Dit betekent dat ook tijdens eventuele stakingen de strafrechtelijke aansprakelijkheid voor het ongestoord functioneren van de desbetreffende voorzieningen overeind blijft."
(TK 1989-1990, 21 551, nr. 3 (MvT), p. 19-20)

14. In de Memorie van Antwoord wordt ingegaan op de kritiek die door de Raad van Centrale Ondernemingsorganisaties op het wetsvoorstel was geuit. Daarbij wordt onder meer gesteld:
"De Raad gaat vervolgens in op in het voorgestelde artikel 161 sexies gemaakte verschil in strafmaat tussen enerzijds de bemoeilijking van de werking van een geautomatiseerd werk ten algemenen nutte en anderzijds het gemeen gevaar voor de verlening van diensten. Hij concludeert daaruit dat het vernielen van de computer van een nutsbedrijf minder erg zou zijn dan dat van bij voorbeeld een bank. Ik meen dat de RCO ten onrechte de verhindering of bemoeilijking van de opslag en verwerking van gegevens ten algemenen nutte op één lijn stelt met het gemeen gevaar voor de verlening van diensten. De structuur van de bestaande en voorgestelde strafbepalingen is aldus dat de aanhef de kern van het strafbaar feit omschrijft en de daaropvolgende onderdelen de strafmaat differentiëren naar gelang de gevolgen die intreden als gevolg van de in de aanhef omschreven gedraging, met dien verstande dat indien geen van de in de onderdelen genoemde gevolgen intreedt, doch uitsluitend het in de aanhef omschreven feit wordt gepleegd, er geen sprake is van strafbaarheid. Het gaat dus om een door het gevolg gekwalificeerd delict De opzet behoeft slechts te zijn gericht op de in de aanhef genoemde gedraging en behoeft niet tevens te zijn gericht op het gevolg.
De RCO nu stelt ten onrechte de verhindering en bemoeilijking van de opslag of verwerking van gegevens op één lijn met het gemeen gevaar voor de verlening van diensten.
Het "gemeen" gevaar ziet, zoals ook blijkt uit het opschrift van Titel VII, waarin de voorgestelde bepaling zal worden ingevoegd, op de algemene veiligheid. Noyon-Langemeijer-Remmelink zegt hierover dat de veroorzaker van het gevaar de omvang van het gevaar vooraf niet kan berekenen of naar willekeur bepalen. Gemeen gevaar voor de verlening van diensten ziet dus op een zodanige stoornis van een geautomatiseerd werk dat vooraf geen inzicht kan worden gevormd over de omvang van de schade die daardoor wordt aangericht. Beperkt de stoornis zich tot een computer die betrekking heeft op een bepaald soort dienstverlening, die door de schade uitvalt, zonder dat verderstrekkende gevolgen kunnen intreden, dan is er geen sprake van gemeen gevaar. Bij dit alles is het van geen belang of de dienstverlening plaatsvindt ten algemenen nutte dan wel binnen een sector van het bedrijfsleven, bij voorbeeld het bankwezen.
De verhindering en bemoeilijking van de opslag of verwerking van gegevens is van een geheel andere orde. Geenszins behoeft daardoor de dienstverlening in gevaar te komen. Evenmin gaat het om een gevaar. Slechts indien daadwerkelijk de opslag of verwerking wordt belemmerd, is er sprake van strafbaarheid. Te denken valt aan een merkbare vertraging in het functioneren van een geautomatiseerd werk of in hinderlijke fouten in het functioneren van de computer die steeds moeten worden hersteld. De reikwijdte van deze strafbepaling is beperkt tot geautomatiseerde werken ten algemenen nutte. Dan is er immers een belang van ruimere strekking dan alleen het belang van de desbetreffende organisatie. Binnen het particuliere bedrijfsleven is men aangewezen op civielrechtelijke middelen, bij voorbeeld het ontslag van het personeel dat de bemoeilijking veroorzaakt. Voor alle duidelijkheid wijs ik erop dat het hier niet gaat om een storing die wordt veroorzaakt doordat programmagegevens worden gewijzigd. Is dit het geval dan wordt het voorgestelde artikel350a overtreden."
(TK 1990-1991, 21551, nr. 6 (MvA), p. 13)

15. In de MvT wordt opgemerkt dat het voorgestelde art. 161sexies aansluit bij de bestaande bepalingen uit Titel VII van Boek 2 van het Wetboek. De in deze Titel opgenomen gemeengevaarlijke delicten zijn er evenwel in soorten en maten. Ik zal dat hierna pogen te verduidelijken. Dit omdat de vraag is bij welke bepalingen in het bijzonder art. 161sexies aansluit. In het verlengde daarvan ligt de vraag hoeveel gewicht moet worden toegekend aan het beroep dat in de MvT en de MvA wordt gedaan op het karakter van de gemeengevaarlijke delicten.

16. Het in de praktijk meest voorkomende en daardoor wellicht gezichtsbepalende gemeengevaarlijke delict is de brandstichting, strafbaar gesteld in art. 157 Sr, waarmee de genoemde Titel VII opent. Het gemeengevaarlijke karakter van dit delict schuilt in de aard van de handeling: brandstichting is gevaarlijk omdat het vuur om zich heen kan grijpen. Het gaat bij de strafbaarstelling dan ook niet om de bescherming van het in brand gestoken object. Dat wordt onderstreept door het feit dat ook iemand die zijn eigen spullen in brand steekt, zich schuldig kan maken aan art. 157 Sr. Want ook dan kan het gevaar bestaan dat de brand overslaat naar andere goederen of dat mensen in de vlammen omkomen. In dat dreigende gevaar vindt de strafbaarstelling haar grond. Brandstichting is dan ook niet strafbaar (althans niet op grond van art. 157 Sr) als dat gevaar objectief gezien niet aanwezig is.

17. In de MvA wordt, met een beroep op Noyon-Langemeijer-Remmelink, gesteld dat "gemeen gevaar voor

de verlening van diensten" ziet "op een zodanige stoornis van een geautomatiseerd werk dat vooraf geen inzicht kan worden gevormd over de omvang van de schade die daardoor wordt aangericht". In Noyon-Langemeijer-Remmelink wordt weer verwezen naar de MvT op art. 157 Sr, waarin ter adstructie van de overeenkomst tussen brandstichting enerzijds en het veroorzaken van een ontploffing of overstroming anderzijds wordt gesteld: "Men brengt eene natuurkracht in werking waarvan de gevolgen niet te berekenen zijn.".(8) Naar mijn mening kan uit deze karakterisering niet worden afgeleid dat strafbaarheid steeds ontbreekt als vooraf duidelijk is wat de (totale) omvang van de schade zal zijn. Dat geldt ook voor brandstichting. Waar het mijns inziens om gaat, is dat vooraf niet te voorzien moet zijn dat de brand beperkt blijft tot het in brand te steken object. Als die voorzienbaarheid ontbreekt, zijn, om met de MvT op art. 157 Sr te spreken, de gevolgen niet te berekenen. Er is dan sprake van gemeen gevaar voor goederen. Dat is niet het geval als wél vooraf te berekenen valt dat het vuur tot het in brand te steken object beperkt blijft. Het stellen van een verdergaande eis - in die zin dat de totale omvang van de brand niet te voorspellen moet zijn - is in strijd met de ratio legis. Stel de dader steekt een hooiberg in brand die op het erf staat van een eenzame boerderij op het godvergeten Groninger platteland. Vooraf staat dan vast dat alleen de boerderij en de daarin aanwezige goederen gevaar kunnen lopen. Waarom zou de strafbaarheid in dat geval moeten afhangen van de vraag hoe zeker het vooraf gezien is dat de brand de hele boerderij in de as zal leggen? Voldoende is dat de kans dat de brand overslaat objectief gezien reëel is. Het is absurd om straffeloosheid aan te nemen als het menselijkerwijs gesproken zo goed als zeker is - doordat de hooiberg zowat tegen het kurkdroge rieten dak van de boerderij aanleunt - dat de hele boerderij met al wat daarin is in vlammen zal opgaan. Of de totale omvang van de schade al dan niet te voorzien valt, doet dus niet terzake.(9)

18. Daar komt dan nog bij dat het in de MvT op art. 157 Sr ging om een karakterisering van de gedragingen die in art. 157 Sr zijn strafbaar gesteld. Er is dus geen goede grond om het gestelde door te trekken naar gemeengevaarlijke delicten die niet bestaan uit het in werking brengen van een natuurkracht.

19. Omdat het gevaar bij brandstichting in de handeling schuilt, is het delict voltooid zodra de brand is gesticht. Dat betekent dat de strafbaarheid niet afhankelijk is van daadwerkelijke schade. Het gevaar behoeft niet te zijn gerealiseerd. De wet eist ook niet dat het in brand gestoken object is vernield, beschadigd of onbruikbaar gemaakt. Om de bescherming van dat object gaat het als gezegd niet. Omgekeerd geldt dat het aanrichten van daadwerkelijke schade nog niet betekent dat de dader zich schuldig heeft gemaakt aan het strafbare feit van brandstichting (art. 157 Sr). In de eerste plaats uiteraard omdat de schade ook op andere wijze dan door brandstichting kan zijn aangericht. In de tweede plaats omdat sprake kan zijn van afzonderlijke brandstichtingen. Wie een hooiberg in de brand steekt, maakt zich schuldig aan art. 157 Sr als het gevaar bestaat dat de brand overslaat naar twee andere zich in de nabijheid bevindende hooibergen. Wie daarentegen drie ver van elkaar in de verlatenheid staande hooibergen in de brand steekt, pleegt niet het strafbare feit van art. 157 Sr, ook al is de schade even groot of groter. Van gemeen gevaar voor goederen is in dat geval geen sprake geweest.

20. Voor de onderhavige casus is dat wellicht niet zonder betekenis. Het enkele feit dat een groot aantal particulieren niet (veilig) meer kan internetbankieren, betekent nog niet dat sprake is geweest van een gemeen gevaar voor de verlening van diensten dat zich heeft gerealiseerd. Als een bende onverlaten plunderend door de stad trekt en met knuppels alle personal computers die zij aantreft, in elkaar slaat, is het effect daarvan dat een grote groep burgers internetbankieren wel even kan vergeten. Maar dat wil niet zeggen dat de groep onverlaten zich schuldig heeft gemaakt aan het medeplegen van art. 161sexies Sr. Van de vernieling van één enkel geautomatiseerd werk (daarop lijkt het artikel het oog te hebben) die tot gevolg heeft dat de dienstverlening gevaar loopt, is geen sprake. Het opgetreden effect is het gevolg van een veelheid van vernielingen, die elk afzonderlijk geen gevaar voor de dienstverlening opleverden.

21. Dat het bij art. 157 Sr niet gaat om de bescherming van het object dat in brand wordt gestoken, brengt ook mee dat het bij het vereiste gemeen gevaar voor goederen niet gaat om de schade die het gevolg kan zijn van de vernieling of de beschadiging van dat object. Een voorbeeld om dat te verduidelijken. Als iemand een vuurtoren in de brand steekt, valt doorgaans objectief te voorzien dat die vuurtoren daardoor zal ophouden te branden met als gevolg dat talloze schepen op zee op de klippen dreigen te lopen. Toch is daarmee de delictsomschrijving van art. 157 Sr niet vervuld. Het gevaar dat de schepen lopen, is namelijk niet het gemeen gevaar voor goederen waarop het artikel het oog heeft. Dat gevaar is dat de brand zal overslaan op andere goederen. En dat gevaar lopen de schepen op zee niet.

22. Er zijn ook gemeengevaarlijke delicten waarbij het wel (primair of zelfs uitsluitend) gaat om de schade die het gevolg is van de vernieling van het desbetreffende object. Men denke bijvoorbeeld aan de vernieling van een elektriciteitscentrale (art. 161bis Sr). Van gemeen gevaar voor goederen is hier bijvoorbeeld sprake als diepgevroren goederen door de stroomuitval dreigen te bederven (HR 10 oktober 1989, NJ 1990, 172). Het gemeen gevaar voor goederen bestaat hier dus niet uit het gevaar dat ook andere elektriciteitscentrales door de vernieling onklaar raken. De vernieling van één centrale is al erg genoeg. Dat wordt onderstreept door het feit dat gemeen gevaar voor goederen of levengevaar voor een ander hier geen noodzakelijke voorwaarde voor strafbaarheid is. Als de vernielde centrale stroom ten algemene nutte levert, is het enkele feit dat de stroomlevering is verhinderd of bemoeilijkt, voldoende voor strafbaarheid (art. 161bis sub 1º Sr).

23. Het verschil vindt zijn verklaring mijns inziens in het feit dat het misdrijf van art. 161bis Sr zijn gemeengevaarlijke karakter niet ontleent aan de gevaarlijkheid van de gedraging, maar aan de beschermenswaardigheid van het betrokken object. De wijze waarop het elektriciteitswerk wordt vernield, doet dan ook niet ter zake. Dat kan brandstichting zijn, maar bijvoorbeeld ook een bombardement. Elke gedraging die tot vernieling van het werk leidt, valt onder de delictsomschrijving. Dat wijst erop dat het in

art. 161bis Sr, anders dan in art. 157 Sr, wél om de bescherming van het object in kwestie gaat. Elektriciteitswerken zijn in onze samenleving van zo'n vitaal belang, dat zij een bijzondere bescherming verdienen. De afhankelijkheid van de samenleving van elektriciteit is zo groot, dat met het tegengaan van stroomuitval een algemeen belang is gemoeid. Die betrokkenheid van het algemeen belang maakt dat het gevaar dat de stroomlevering ten algemene nutte uitvalt als een gemeen gevaar kan worden bestempeld.

24. Het belang van een ongestoorde stroomvoorziening (dat in art. 161bis Sr bescherming vindt), maakt voorts dat het "gemeen gevaar voor goederen" waarvan het artikel spreekt, een eigen inhoud krijgt. Het gaat om het gevaar dat goederen lopen doordat de stroomvoorziening uitvalt. Het voorbeeld van de in brand gestoken vuurtoren kan hier nogmaals dienstig zijn. Van gemeen gevaar voor goederen in de zin van art. 157 Sr was, zo zagen wij, in het voorbeeld geen sprake. Een ramp is dat niet. De vernieling van een vuurtoren valt onder art. 166 Sr en levert dus een apart gemeengevaarlijk delict op. Het gevaar dat schepen stranden, zou bij dat delict wél "gemeen gevaar voor goederen" hebben opgeleverd, zij het dat de wetgever dat gevaar specifieker heeft omschreven, namelijk als "gevaar voor de veiligheid van de scheepvaart".

25. Het is de eigen, wisselende inhoud die het vereiste van te duchten gevaar bij de verschillende gemeengevaarlijke delicten heeft, die maakt dat het hachelijk is om, zoals in de MvA met betrekking tot art. 161sexies Sr is gedaan, het begrip gemeen gevaar zoals dat in het kader van art. 157 Sr functioneert, te veralgemeniseren en daaruit conclusies te trekken met betrekking tot andere delicten (vergelijk hiervoor, punt 17). Op grond van die benadering wordt zoals wij zagen in de MvA gesteld dat er geen sprake is van gemeen gevaar als "de stoornis zich [beperkt] tot een computer die betrekking heeft op een bepaald soort dienstverlening, die door de schade uitvalt, zonder dat verderstrekkende gevolgen kunnen intreden."(10) Als in de MvA aansluiting was gezocht bij het type gemeengevaarlijke delicten waarvan sprake is in art. 161bis en art. 166 Sr, had deze beperkte uitleg allerminst voor de hand gelegen. Een elektriciteitscentrale beperkt zich maar tot één bepaald soort dienst, namelijk de levering van stroom. Toch wordt de storing in de stroomvoorziening als een gemeen gevaar beschouwd. Ook de functie van een vuurtoren is nogal eenzijdig. Toch kan de vernieling van die vuurtoren gevaar voor de veiligheid van de scheepvaart opleveren. Als naar analogie daarvan wordt geredeneerd, valt niet goed in te zien waarom niet van een gemeen gevaar voor de verlening van diensten kan worden gesproken als de vernieling van een computer die maar één (vitale) functie vervult (zoals het faciliteren van internetbankieren), tot gevolg heeft of dreigt te hebben dat de daarmee gemoeide dienstverlening niet meer mogelijk is.

26. Een belangrijke vraag is gelet op het voorgaande om welk type gemeengevaarlijk delict het in art. 161sexies Sr gaat. Gaat het om het ontketenen van (natuur)krachten die niet in de hand zijn te houden of gaat het om het vernielen, beschadigen (enz.) van installaties die in de maatschappij een cruciale functie vervullen? Er kan mijns inziens weinig twijfel over bestaan dat het laatste het geval is. Daarop wijst in de eerste plaats de reden voor strafbaarstelling die in de MvT wordt genoemd. Zoals wij zagen, wordt die reden gezocht in "de plaats die de geautomatiseerde opslag, verwerking en overdracht van gegevens in de samenleving is gaan innemen". Bedoeld lijkt te zijn dat de toenemende afhankelijkheid van de samenleving van die geautomatiseerde opslag en verwerking maakt dat daarmee algemene belangen zijn gemoeid en dat daarom strafbaarstelling als gemeengevaarlijk delict gerechtvaardigd is. Daarop wijst in de tweede plaats de vermelding in de MvT dat de voorgestelde artikelen 161sexies en 161septies (de schuldvariant van art. 161sexies) op dezelfde leest zijn geschoeid als de artikelen 161bis en 161ter. Daarop wijst in de derde plaats de tekst van art. 161sexies Sr, die inderdaad grote gelijkenis vertoont met die van art. 161bis Sr. Strafbaar is dan ook niet gesteld het op een specifieke wijze ontketenen van niet in de hand te houden (natuur)krachten (zoals het 'loslaten' van wormen op internet) waardoor gemeen gevaar voor het naar behoren functioneren van geautomatiseerde werken te duchten is, maar het vernielen (enz.) van enig geautomatiseerd werk. De wijze waarop de vernieling plaatsvindt (door brandstichting of anderszins) is daarbij onverschillig.

27. Een verschil met art. 161bis Sr is wel dat het begrip "enig geautomatiseerd werk" in art. 161sexies Sr ruim lijkt te zijn begrensd. Wat onder "enig electriciteitswerk" moet worden verstaan, is te vinden in art. 90ter Sr. Het moet gaan om "werken dienende tot voortbrenging, geleiding, transformatie of levering van elektriciteit en daarmede in verband staande beveiligings-, ondersteunings- en waarschuwingswerken". Deze begripsomschrijving maakt duidelijk dat het moet gaan om werken die ervoor zorgen dat de klant (huishoudens en bedrijven) van stroom wordt voorzien. Tot die werken behoort nog wel de meterkast, maar niet het koffiezetapparaat en de vaatwasmachine. Dat de vernieling van alle elektrische apparaten in een bepaald huishouden voor de betrokkenen even erg - of zelfs erger - is dan de vernieling van de meterkast, maakt nog niet dat de stroomvoorziening daardoor in gevaar is gebracht. Dat van die stroomvoorziening geen gebruik kan worden gemaakt, is een andere zaak. De duidelijkheid die art. 90ter Sr met betrekking tot art. 161bis Sr biedt, moet art. 161sexies Sr ontberen. Toch lijkt een analoge wetsuitleg gelet op de ratio legis geboden. Anders zou de vernieling (enz.) van een personal computer die door de klant wordt gebruikt om de op internet aangeboden diensten af te nemen, het gemeengevaarlijke delict van art. 161sexies Sr opleveren.

28. De gewenste beperking kan daarbij niet gevonden worden in een beperkte uitleg van het begrip "enig geautomatiseerd werk" als zodanig, maar in de uitleg van het "gemeen gevaar" dat van de vernieling (enz.) van een dergelijk werk te duchten moet zijn. Die uitleg brengt mee dat het in art. 161sexies lid 1 sub 2 º en sub 3 º Sr moet gaan om geautomatiseerde werken die een (cruciale) functie vervullen bij hetzij de beveiliging van personen of goederen, hetzij bij de verlening van diensten. Als dat niet het geval is kan van de vernieling van die werken geen gemeen gevaar voor goederen, levensgevaar voor een ander of gemeen gevaar voor de verlening van diensten te duchten zijn.

29. Steun voor deze benadering is te vinden in HR 2 december 1997, NJ 1998, 306, waarin het ging om

iemand die dreigde de computer van een makelaarskantoor op de grond te gooien. Dat daardoor mogelijk ook andere, zich in de nabijheid bevindende goederen gevaar liepen, was onvoldoende om gemeen gevaar voor goederen aan te nemen. De Hoge Raad overwoog dat de wetgever blijkens de wetsgeschiedenis bij art. 161sexies Sr "ook voor wat de strafbaar gestelde vernieling, beschadiging of onbruikmaarmaking van het desbetreffende werk betreft, het oog [heeft] gehad op het gemeen gevaar voor goederen dat is te duchten van daardoor optredende verstoring van het functioneren van dat werk". Het moet dus gaan om (gevaar voor) goederen die door (het functioneren van) de computer worden beschermd. (11)

30. In de hier verdedigde wetsuitleg - waarin de functie van de desbetreffende computer bepalend is voor de vraag of van gemeen gevaar kan worden gesproken - komt veel gewicht toe aan het feit dat in art. 161sexies Sr gesproken wordt van de "verlening" van diensten (en niet van het gebruik van diensten). Van gemeen gevaar voor de verlening van diensten kan alleen sprake zijn als de computer in kwestie een functie vervult bij de verlening van diensten.

31. Ik merk op dat deze uitleg recht doet aan de verhouding tussen art. 161sexies lid 1 sub 1º en art. 161sexies lid 1 sub 2º Sr zoals die in de MvA is toegelicht (hiervoor, punt 13). De verschillende strafbaarstellingen (sub 1º en sub 2º) zijn onmiskenbaar geschoeid op de leest van art. 161bis Sr en de in de MvA gegeven toelichting bevestigt dat hun onderlinge verhouding dezelfde is. Als het gevolg van de vernieling (enz.) van een geautomatiseerd werk enkel is dat de opslag, verwerking of overdracht van gegevens (wederrechtelijk) wordt bemoeilijkt of verhinderd, levert die vernieling (enz.) alleen een gemeengevaarlijk delict op als het gaat om opslag, verwerking en overdracht "ten algemene nutte". De MvA verwoordt dit door te stellen: "De reikwijdte van deze strafbepaling is beperkt tot geautomatiseerde werken ten algemene nutte" (curs. van mij, Kn). Als rechtvaardiging voor die beperking wordt genoemd dat er "dan immers een belang [is] van ruimere strekking dan alleen het belang van de particuliere organisatie". De (veel) zwaardere strafbaarstelling van art. 161sexies lid 1 sub 2º Sr vindt haar rechtvaardiging in het gevaar dat te duchten is. Dat gevaar maakt dat het niet per se hoeft te gaan om de vernieling (enz.) van een geautomatiseerd werk ten algemene nutte. Ook de vernieling van een computer die onderdeel vormt van het geautomatiseerde beveiligingssysteem van een particuliere organisatie kan daar bijvoorbeeld onder vallen. Hetzelfde geldt wellicht voor een computer die wordt gebruikt voor de interne dienstverlening binnen een bepaalde organisatie, waarbij bijvoorbeeld te denken valt aan een geautomatiseerde personeelsadministratie waarin werknemers zelf hun verlofdagen kunnen registreren. De vernieling van een computer waarmee van de op internet aangeboden diensten gebruik gemaakt kan worden, kan daarmee bezwaarlijk op één lijn gesteld worden. Het belang van de particuliere computerbezitter om te kunnen internetten, ligt in dezelfde orde van grootte als zijn belang om met zijn computer gegevens te kunnen verwerken en op te slaan. In elk geval valt niet in te zien dat hier opeens wél sprake is van een belang van "ruimere strekking", laat staan van een zo zwaarwegend belang dat strafbaarstelling op basis van art. 161sexies lid 1 sub 2º Sr is gerechtvaardigd.

32. Aandacht bij dit alles verdient dat het verstoren van het (particuliere) computergebruik niet straffeloos is als het begrip "gemeen gevaar" in art. 161sexies Sr beperkt wordt uitgelegd. In de aangehaalde passage uit de MvA wordt daar "voor alle duidelijkheid" op gewezen. De 'ouderwetse' vernieling, beschadiging of onbruikbaar making van de computer door fysiek geweld is strafbaar op grond van art. 350 Sr. Als de storing van het normale gebruik het gevolg is van geknoei met de software (het wissen, onbruikbaar of ontoegankelijk maken van de opgeslagen of verwerkte gegevens of het daaraan toevoegen van andere gegevens), is de dader strafbaar op grond van art. 350a Sr. Daarbij voorziet het tweede lid in strafverzwaring als het geknoei met de software geschiedt na binnendringing door tussenkomst van een openbaar telecommunicatienetwerk en daarbij "ernstige schade met betrekking tot [de] gegevens" is veroorzaakt.(12) Of het feit dat niet meer veilig kan worden getelebankierd als dergelijke ernstige schade kan worden aangemerkt, is een vraag die hier niet behoeft te worden beantwoord.(13)

33. In punt 24 merkte ik op dat het 'loslaten' van wormen op internet niet het gemeengevaarlijke delict van art. 161sexies Sr oplevert. Dat vindt bevestiging in het feit dat dergelijk gevaarzettend gedrag strafbaar is gesteld in art. 350a lid 3 Sr. Het artikellid voorziet volgens de Nota van wijziging in "de strafbaarstelling van de verspreiding van virussen, ook wanneer deze nog niet daadwerkelijk schade hebben aangebracht".(14)

34. Een bijkomend argument kan voorts nog gevonden worden in de invoeging in het Wetboek van Strafrecht van art. 138b Sr bij Wet van 1 juni 2006, Stb. 300 (Wet computercriminaliteit II).(15) In dat artikel wordt 'bombing' (een speciale vorm van spam) strafbaar gesteld. In de MvT wordt daarover het volgende opgemerkt:
" Onder spam worden verschillende gedragingen verstaan met verschillende gevolgen. De "klassieke" vorm is het ongevraagd toezenden van een e-mail aan een groot aantal personen. Vaak gebeurt dit voor reclamedoeleinden (direct marketing). Daarnaast is er het toezenden van een grote hoeveelheid e-mail (inhoud vaak niet relevant, bijvoorbeeld tienmaal de bijbel) aan één persoon met als doel dat diens e-mailbox verstopt raakt waardoor hij geen e-mails meer kan ontvangen. Dit wordt ook wel bombing genoemd. In zo'n geval is de beschikbaarheid (availability) van een Internetdienst voor individuele gebruikers in het geding. Dergelijke bombardementen van e-mails kunnen dusdanig ernstige vormen aannemen dat zelfs de werking van de server van een Internet Service Provider tijdelijk wordt verstoord en daardoor diens dienstverlening ernstig wordt bemoeilijkt. In zo'n geval kan sprake zijn van het strafbaar feit van artikel 161sexies (onderdeel 1) of artikel 161septies (onderdeel 1) Sr: het (opzettelijk dan wel culpoos) vernielen, beschadigen, onbruikbaar maken, stoornis in de werking veroorzaken enz., van een geautomatiseerd werk, waardoor wederrechtelijk verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst ontstaat.

Ik meen, mede gelet op de genoemde maatschappelijke signalen, dat het wenselijk is ook die gevallen van spam (of bombing) strafbaar te stellen, waarin weliswaar niet de werking van een compleet netwerk of complete telecommunicatiedienst wordt verstoord maar wel de toegang van een individuele gebruiker tot zo'n netwerk of dienst wordt belemmerd. In zo'n geval wordt immers een elementair rechtsgoed in gevaar gebracht, namelijk de mogelijkheid van eenieder om ongehinderd gebruik te maken van een in de moderne samenleving belangrijk communicatiemedium."
(TK 1998-1999, 26671, nr. 3, p. 40)

Volgens deze MvT komt art. 161sexies Sr ingeval van bombing pas in beeld als de werking van de server van een Internet Service Provider daardoor tijdelijk wordt verstoord "en daardoor diens dienstverlening ernstig wordt bemoeilijkt". De toegang van de individuele gebruiker tot het internet (en daarmee de mogelijkheid om van de daarop aangeboden diensten gebruik te maken) is een belang dat door een aparte strafbaarstelling moet worden beschermd.

35. Mijn slotsom is dat van gemeen gevaar voor de verlening van diensten alleen sprake kan zijn ingeval van vernieling (enz.) van een geautomatiseerd werk dat bij de dienstverlener ten behoeve van diens dienstverlening in gebruik is. Dat betekent dat het middel op een onjuiste rechtsopvatting berust en daarom niet kan slagen.

36. Enigszins buiten de orde (het middel heeft daarop geen betrekking) nog een opmerking over de vraag welke betekenis moet worden toegekend aan het in art. 161sexies Sr gehanteerde meervoud (diensten). Mijns inziens komt, in weerwil van hetgeen in de MvA werd gesteld, bij de uitleg van het bestanddeel "gemeen gevaar voor de verlening van diensten" noch aan de onvoorspelbaarheid van de schade, noch aan het al dan niet meervoudige karakter van de dienstverlening enige betekenis toe. Dit omdat, naar hiervoor is uiteengezet, het gestelde in de MvA berust op een ondeugdelijke vergelijking met art. 157 Sr. Niet noodzakelijk is dus dat de vernielde computer meer dan een soort dienst verleent. Voor zover aan het gebezigde meervoud enige betekenis moet worden toegekend, is die betekenis dat de dreigende verstoring van de dienstverlening enige omvang moet hebben. Als het manipuleren van de computer van de dienstverlener slechts tot gevolg heeft dat de desbetreffende dienst aan één klant niet (behoorlijk) kan worden verleend, is van gemeen gevaar wellicht geen sprake.

37. Het middel faalt.

Het middel van de verdachte
38. Het middel van de verdachte klaagt over het oordeel van het Hof dat ten aanzien van het onder 1 tenlastegelegde en bewezenverklaarde sprake was van "het doorbreken van een beveiliging" en "een technische ingreep".

39. Het middel bouwt voort op een in feitelijke aanleg gevoerd verweer. Het Hof heeft dat verweer verworpen en daartoe onder meer het volgende overwogen:
" D1.
Zijdens verdachte is door de raadsman ter terechtzitting in hoger beroep bepleit dat verdachte wordt vrijgesproken van het onder 1 ten laste gelegde nu niet bewezen kan worden dat een (minimale) beveiliging is doorbroken dan wel dat een technische ingreep gepleegd is door verdachte en/of zijn medeverdachte, zoals, aldus de verdediging, vereist op grond van artikel 138a van het Wetboek van Strafrecht.

D2.
Het hof overweegt hiertoe het volgende.
Op grond van het verhandelde ter terechtzitting in hoger beroep stelt het hof onder meer het volgende vast.
(bijlage A000:)
(...)

l. In een testopstelling werd deze bot getest en werden de functionaliteiten beschreven. In een aanvullend proces-verbaal van 17 juli 2008 van verbalisanten [verbalisant 1] en [verbalisant 2] wordt een nadere omschrijving gegeven van de computers die zijn gebruikt in deze testopstelling (Het hof: zie hierna).
(Aanvullend proces-verbaal 17 juli 2008:)
m. In de testopstelling werden computers gebruikt die waren voorzien van het besturingssysteem Windows XP. Gebruikers van Windows XP kunnen er voor kiezen om dit systeem automatisch te laten voorzien van updates. Periodiek worden deze updates cumulatief aangeboden, zodat gebruikers ook in één keer alle updates kunnen installeren. Deze cumulatieve updates worden ook wel servicepacks genoemd. Ten tijde van het onderhavige onderzoek waren er reeds twee servicepacks, te weten Service Pack 1 (september 2002) en Service Pack 2 (augustus 2004). Het infecteren door de Toxbot blijkt te geschieden door het doorbreken van een beveiliging in Windows (XP) systemen die niet zijn voorzien van servicepack 2. Deze vorm van infectie is nagebootst in de testopstelling.
n. Door middel van deze infectiemethode kan het Toxbot virus een systeem binnendringen en zich daar nestelen als een programma. Om zich op deze manier als programma in een systeem als Windows te nestelen zijn 'administrator' of 'SYSTEM' rechten vereist op de betreffende computer.
o. Een standaard Windows XP installatie is beveiligd tegen het inloggen van buitenaf om daar vervolgens door middel van het gebruik van SYSTEM en/of administrator rechten programma's op te installeren.
(rapportage [verbalisant 1] 26 augustus 2008:)
p. Het Windows XP systeem is voorzien van talloze beveiligingen om onbevoegden van het systeem te weren. Het ontwikkelen van de updates en periodieke servicepacks is een reactie op de manieren die ontwikkeld zijn

door hackers om deze beveiligingen te doorbreken of te omzeilen.
q. Uitgaande van het gegeven dat Windows XP standaard is voorzien van beveiliging is er voor gekozen om in de testopstelling gebruik te maken van XP systemen die niet zijn voorzien van updates of servicepacks. Temeer ook, omdat virussen als Toxbot zich juist richten op deze PC's.
r. In 2003 werden manieren ontdekt om via ingangen van hidden shares een beveiliging te doorbreken. Door middel van het opzettelijk geven van verkeerde signalen aan delen van het Windows besturingssysteem van PC's kan een systeem dusdanig in de war raken dat delen tijdelijk onbruikbaar raken of zelfs crashen. Dit is ook waargenomen bij de werking van het Toxbotvirus.
s. Om te voorkomen dat een (Toxbot)virus direct wordt gedetecteerd door een virusscanner wordt door hackers een techniek genaamd packing gebruikt. Deze techniek zorgt ervoor dat het virus wordt 'ingepakt' in een gecomprimeerd en versleuteld bestand, waardoor het ondetecteerbaar blijft voor virusscanners.
(Proces-verbaal BI.2:)
t. Op 2 augustus 2005 wordt via afgetapte internetdata bij verdachte waargenomen dat op 28 juli 2005 een update commando werd gegeven door [verdachte] aan het botnetwerk. Dit commando hield in dat de geïnfecteerde computers in het botnetwerk de opdracht krijgen om ergens op het internet een nieuwe bot, genaamd tox.exe te downloaden en starten.
u. Het bestand tox.exe is door verbalisant [verbalisant 1] uitgevoerd op een computer met het Windows besturingssysteem. Het programma tox.exe bleek een nieuw uitvoerbaar programma met de naam mapi32.exe aan te maken. Het bestand bleek te zijn versleuteld en gecomprimeerd (ofwel gepackt) zoals in de rapportage van 26 augustus 2008 is omschreven, om herkenning door virusscanners te voorkomen.
v. Na het scannen van dit bestand met een antivirusprogramma werd de bot geïdentificeerd als de W32.Toxbot.

D3.
Bij de beoordeling van dit ten laste gelegde feit is de juiste uitleg van de woorden "wederrechtelijk binnendringen" van belang. Het hof heeft daartoe gezocht naar de bedoeling van de wetgever. Van wederrechtelijk binnendringen in de zin van artikel 138a van het Wetboek van Strafrecht is sprake indien men zich de toegang verschaft tegen de onmiskenbare wil van de rechthebbende, welke zowel uit woorden als uit daden kan blijken.
Zoals uit de wetsgeschiedenis blijkt kan daarbij worden gedacht aan het plaatsen van een tekst op het beeldscherm dat toegang voor onbevoegden verboden is. Maar omdat deze woorden een per ongeluk tot stand gekomen toegang niet uitsluiten, bevat voornoemd artikel 138a onder meer ook het aanvullende vereiste dat sprake moet zijn van enige beveiliging, ofwel een kenbare drempel zodat onbevoegden zich niet simpelweg de toegang kunnen verschaffen. (Tweede Kamer, vergaderjaar 1991-1992, 21 551, nr. 11, pagina 18). Artikel 138a verlangt niet meer dan een minimale, doch wel daadwerkelijke beveiliging. Met andere woorden; indien het slachtoffer van computervredebreuk kan aantonen dat er sprake is van enige reële beveiliging dan is dat voldoende. (Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pagina 16).

D4.
Het hof leidt uit de vorenstaande onder Dl. ad m. tot en met q. opgenomen feiten en omstandigheden af dat iedere versie van Windows XP, zodra een particulier die aankoopt, is uitgerust met (een standaard) beveiliging. Naar het oordeel van het hof is hierbij sprake van enige reële beveiliging zoals hiervoor onder D3. is beschreven. Met betrekking tot deze beveiliging acht het hof tevens de rapportage van verbalisant [verbalisant 1] van 26 augustus 2008 van belang, waar deze het volgende inhoudt:

"Als het gaat om een belangrijke beveiliging van XP in een netwerkomgeving als internet, is het volgende punt in dit verband het belangrijkste voorbeeld: Windows XP is een Windows variant uit de zogenaamde 'NT' familie, ontstaat uit Windows NT3.5 opgevolgd door Windows NT4.0, Windows 2000, Windows XP en Windows Vista. In de versies tot en met Windows 2000 was het in sommige gevallen mogelijk om deze via het netwerk te benaderen en er met gebruikmaking van Administratonechten bestanden naar toe te sturen en zelfs uit te voeren. De genoemde methode maakte gebruik van de standaard door Windows aangemaakte verborgen shares als C$ en ADMIN$. Microsoft heeft deze optie van administrator toegang bij de introductie van XP bewust geblokkeerd en actief deze manier van niet-geautoriseerd gebruik beveiligd door deze toegang van buitenaf gebruik te laten maken van de geminimaliseerde rechten van het standaard aanwezige 'Guest' account. Een dergelijk Guest account heeft onvoldoende systeemrechten om die dingen te doen die door middel van het Toxbot virus wel worden gedaan. ( ) Het blokkeren van de verborgen shares nam voor anderen de laatste mogelijkheid weg om via het netwerk administrator rechten te verkrijgen zonder actief een beveiliging te doorbreken. In 2003 werden manieren ontdekt om via de oude ingangen van de hidden shares toch toegang te verkrijgen.".

Voorts blijkt uit hetgeen onder D1. ad r. tot en met u. is opgenomen dat verdachte het virus zodanig versleutelde en comprimeerde (het zogenoemde packing), dat het betreffende systeem het virus niet als een fout herkende. Het virus verspreidde zichzelf vervolgens als een 'worm' middels de besmette computer naar andere computers. Deze werkwijze houdt naar het oordeel van het hof niets anders in dan dat verdachte niet alleen gaten in systeembeveiliging opzocht ten einde als administrator/system en aldus onder een valse hoedanigheid in de zin van artikel 138a van het Wetboek van Strafrecht, binnen te dringen, maar zich daarbij tevens bediende van een technische ingreep met behulp van valse signalen, te weten door in dit geval verhuld en onherkenbaar, middels het 'verpakte' virus binnen te dringen.
Gelet op de gehanteerde werkwijze, als hiervoor weergegeven is het hof van oordeel dat er sprake is van het doorbreken van de systeembeveiliging en van het verwerven van toegang middels een technische ingreep (tegen de onmiskenbare wil van de rechthebbende) als bedoeld in artikel 138a van het Wetboek van Strafrecht.

D5.
Gelet op het vorenstaande onder D4 overwogene waren ook de versies van vóór Windows XP (onder meer Windows NT 3.5, Windows NT 4.0 en Windows 2000) voorzien van een minimale (standaard) beveiliging. Het vorenstaande heeft derhalve ook te gelden voor zover is binnengedrongen in Windows systemen anders dan Windows XP.

Het hof verwerpt in zoverre het verweer."

40. Het Hof heeft de verdachte veroordeeld wegens het "medeplegen van computervredebreuk meermalen gepleegd", en heeft daarbij bewezenverklaard, zoals hiervoor onder 5 is weergegeven, dat de verdachte in computers is "binnengedrongen, waarbij hij, verdachte en zijn medeverdachte de beveiliging hebben doorbroken, in elk geval de toegang hebben verworven door een technische ingreep, met behulp van valse signalen en/of door het aannemen van een valse hoedanigheid". De verschillende, in deze bewezenverklaring opgenomen onderdelen stemmen overeen met de onder a en b in art. 138a, eerste lid, Sr (oud; zie hiervoor onder 6) opgenomen wijzen van binnendringen of verwerven van toegang. Alleen het gebruik van een valse sleutel komt in de bewezenverklaring niet voor.

41. Het middel van de verdachte lijkt zich niet te richten tegen de oordelen van het Hof dat sprake was van het verwerven van toegang met behulp van valse signalen dan wel door het aannemen van een valse hoedanigheid. Ik heb mij afgevraagd of dit betekent dat het middel reeds om deze reden niet tot cassatie zou kunnen leiden. Ik zou deze vraag niet, althans niet op voorhand, bevestigend willen beantwoorden. In de eerste plaats lijkt, althans op het eerste gezicht, sprake van een alternatieve bewezenverklaring. Volgens vaste jurisprudentie is vereist dat alle bewezenverklaarde alternatieven steun vinden in de bewijsmiddelen. Dat brengt mee dat erover geklaagd kan worden dat twee van de vier alternatieven geen steun vinden in de bewijsmiddelen. In de tweede plaats lijkt het oordeel van het Hof dat sprake is geweest van het gebruik van valse signalen en/of een valse hoedanigheid nauw verweven te zijn met zijn (slot)oordeel onder D4 dat sprake was "van het doorbreken van de systeembeveiliging en van het verwerven van toegang middels een technische ingreep". De tegen dat oordeel gerichte klacht richt zich dan indirect ook tegen de daaraan ten grondslag liggende oordelen met betrekking tot de valse signalen en de valse hoedanigheid.

42. Het middel werpt twee nauw samenhangende vragen op. De eerste is wat verstaan moet worden onder de verschillende begrippen die in art. 138a lid 1 (oud) Sr onder a. en b. worden gebezigd. Wat bijvoorbeeld is het doorbreken van een beveiliging en waarin verschilt dat van een technische ingreep? De tweede vraag is hoe al deze begrippen zich tot elkaar verhouden. Gaat het om onderling scherp afgebakende begrippen of juist om begrippen die weinig vast zijn omlijnd en die elkaar goeddeels overlappen? Beantwoording van die vragen vergt kennis van de totstandkomingsgeschiedenis van art. 138a Sr.

43. In het oorspronkelijke wetsvoorstel dat in 1993 leidde tot de invoeging van art. 138a in het Wetboek van Strafrecht bij de Wet computercriminaliteit, luidde het artikel als volgt:
"1. Hij die wederrechtelijk binnendringt in een daartegen beveiligd geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een daartegen beveiligd deel daarvan, wordt gestraft met gevangenisstraf van ten hoogste drie maanden of geldboete van de tweede categorie.
2. Hij die zich de toegang heeft verschaft door middel van het aannemen van een valse hoedanigheid, listige kunstgrepen of een valse sleutel, wordt geacht te zijn binnengedrongen."

De tekst was gelijkluidend aan die in het rapport van de Commissie Franken waarop het wetsvoorstel was gebaseerd.(16) Zowel in het rapport als in de MvT werd het nieuw te creëren delict aangeduid als "computervredebreuk". Dit omdat het delict verwant zou zijn aan de in art. 138 Sr strafbaar gestelde huisvredebreuk. De terminologie en de opbouw van het voorgestelde art. 138a vertonen niet voor niets grote overeenkomst met die van art. 138 Sr. Dat geldt ook voor het tweede lid, dat is geïnspireerd door art. 138 lid 2 Sr.

44. Over de beveiligingseis is tijdens de parlementaire behandeling het nodige te doen geweest. Dat is niet onbegrijpelijk. Dat moet binnengedrongen zijn "in een daartegen beveiligd" werk is een eis die art. 138 Sr niet kent. Van binnendringen in een woning is al sprake als tegen de verklaarde wil van de bewoner wordt binnengetreden. De woning behoeft dus niet door middel van slot en grendel te zijn afgesloten. De vraag is dan ook wat de in het voorgestelde art. 138a opgenomen beveiligingseis toevoegt aan het daarnaast gestelde vereiste dat de dader wederrechtelijk in het geautomatiseerde werk moet zijn binnengedrongen. Daarbij komt dat binnendringen in een daartegen beveiligd werk iets van een contradictio in terminis heeft. Als is binnengedrongen, was het werk daartegen klaarblijkelijk niet (afdoende) beveiligd. Dat lijkt, merk ik alvast op, ook de teneur van het in deze zaak voorgestelde middel te zijn. Omdat de desbetreffende computers met het W32.Toxbot-virus konden worden geïnfecteerd, waren die computers daartegen kennelijk niet beveiligd, zodat die beveiliging ook niet doorbroken kan zijn.

45. De gesignaleerde onduidelijkheid zette zich voort in het voorgestelde tweede lid. Puur tekstueel gezien zegt dat artikellid, evenals art. 138 lid 2 Sr waaraan het was ontleend, alleen iets over de vraag of is binnengedrongen, dus over de vraag of het zich toegang verschaffen tot de opgeslagen gegevens geschiedde tegen de wil van de rechthebbende. Dat dit het geval is, zegt, als het artikellid letterlijk wordt gelezen, niets over de vraag of binnengedrongen is in een beveiligd werk. Of het onbevoegde gebruik van het (juiste) password het strafbare feit van art. 138a Sr zou opleveren, was dus nog maar de vraag. Er mag dan gebruikgemaakt zijn van een valse sleutel, maar dat wil - uitgaande van een letterlijke lezing - niet zeggen

dat het werk tegen binnendringen is beveiligd. Het afschermen van de opgeslagen gegevens door middel van inlogcodes is mogelijk geen (afdoende) beveiliging. Dat is, zo merk ik alvast op, ook de opvatting te zijn die aan het voorgestelde middel ten grondslag ligt.

46. Nu is de vraag of de bedoelde letterlijke lezing door de ontwerpwetgever was bedoeld. In het rapport van de Commissie Franken wordt gesteld dat op twee manieren zou kunnen blijken dat de toegang tot de gegevens is verschaft tegen de onmiskenbare wil van de rechthebbende: door woorden en door daden.(17) Woorden alleen waren volgens het rapport niet voldoende. Als voorbeeld wordt genoemd een tekst op het beeldscherm als 'verboden toegang voor onbevoegden'. De wil van de rechthebbende moest ook uit daden blijken: "Men denke hier aan wachtwoorden, PIN-codes en dergelijke". Deze verdergaande eis moest volgens de Commissie worden gesteld omdat alleen een bordje "verboden toegang" niet zou uitsluiten dat men "per ongeluk" toegang tot de gegevens zou krijgen.(18) Bij een "hogere drempel" zou dit gevaar zich minder vaak voor doen. Die hogere drempel diende te bestaan "uit bepaalde, tegen het wederrechtelijk binnendringen gerichte, beveiligingsmaatregelen". Aldus werd een "nadere beperking" aangebracht.

47. De Commissie lijkt op twee gedachten te hebben gehinkt. Enerzijds wordt gesteld dat de beveiligingseis een nadere beperking meebrengt (die dus bovenop de eis komt dat tegen de onmiskenbare wil van de rechthebbende wordt gehandeld), anderzijds wordt de beveiligingseis juist gepresenteerd als een uitvloeisel van de eis dat het kennisnemen van de gegevens tegen de onmiskenbare wil van de rechthebbende plaatsheeft. Die eis preciseert dan slechts de vereiste "onmiskenbaarheid" van de wil. Die laatste gedachte is mijns inziens overheersend geweest. Ten aanzien van het voorgestelde tweede lid merkt de Commissie op: "De formulering is zo dat diverse manieren om toegangsbeveiligingen te doorbreken, dan wel te omzeilen, er onder te brengen zijn.". Het gebruik van bijvoorbeeld een valse sleutel wordt hier dus gepresenteerd als een manier om de toegangsbeveiliging te doorbreken. Dat impliceert dat een geautomatiseerd systeem dat door middel van een password is afgeschermd, een tegen binnendringen beschermd werk is als bedoeld in het eerste lid van het voorgestelde art. 138a Sr. Aannemelijk is zogezien dat het voorgestelde tweede lid als volgt gelezen moest worden: "Hij die [enz.] wordt geacht te zijn binnengedrongen in een daartegen beveiligd geautomatiseerd werk".

48. De Commissie stelde een beperkte strafbaarstelling voor. Het strafbaarstellen van het zich onbevoegd toegang verschaffen als zodanig zou leiden tot "overcriminalisering".(19) Tegen die achtergrond moet de gestelde beveiligingseis worden bezien. Daartegen rees, zo blijkt uit de MvT, nogal wat bezwaar.(20) Gevreesd werd dat de slachtoffers van computercriminaliteit geen aangifte zouden doen als hun wijze van beveiliging in de rechtszaal zou worden gekritiseerd door de verdediging. De Minister zag daarin geen reden om van het voorstel van de Commissie af te wijken. Hij lichtte dat standpunt toe door onderscheid te maken tussen absolute, maximale, adequate, minimale en pro forma beveiliging. Naar zijn zeggen volstond minimale beveiliging. Die minimale beveiliging moest daarbij wel een daadwerkelijke zijn. In dat verband werd gesteld: " Dit betekent dat, indien het slachtoffer van een computerinbraak kan aantonen dat er sprake was van enige reële beveiliging, dit voldoende is. Niet is nodig dat deze beveiliging ook adequaat was in het licht van de te beveiligen, aan de gegevens verbonden belangen. Onvoldoende is evenwel pro forma beveiliging. Ik doel hiermee op een beveiliging die geen daadwerkelijke beveiliging is, doch slechts is aangebracht met het oog op bij voorbeeld het ontstaan van strafbaarheid van "hackers".
Wat als minimale beveiliging moet worden aangemerkt is geen statisch, eens en voor altijd vast te stellen gegeven. Het inbreken in een geautomatiseerd werk en het beveiligen van gegevens maken deel uit van een voortdurende elektronische oorlogsvoering. Wat bij een bepaalde stand van de techniek als een adequate beveiliging kan worden gezien, is dat bij een verdere ontwikkeling niet meer. Zo kan ook een beveiliging die op enig moment nog wel als minimaal kan worden aangemerkt, na verloop van tijd zo achterhaald zijn, dat deze niet meer als reëel valt aan te merken.
Het gaat er om dat de 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.
Het bezwaar dat door deze beveiligingseis bedrijven op zakelijke gronden nog meer weerhouden zullen worden aangifte te doen, treft naar mijn oordeel onder deze omstandigheden geen doel. Het kan voor bedrijven geen bezwaar zijn aan te tonen dat zij ten minste enige reële beveiliging hebben, al was het maar dat zij een systeem van autorisatie hebben wat betreft de verlening van toegang. Een dergelijk systeem is algemeen bekend. Daar komt bij dat, indien daadwerkelijk een beveiliging is doorbroken, het in het algemeen van weinig werkelijkheidszin getuigt aan te nemen dat de wetenschap hieromtrent beperkt blijft tot de verdachte. Juist in kringen van computerfanatici, op wier conto in de regel dergelijke inbraken moeten worden geschreven, worden de moderne mogelijkheden om informatie snel te verspreiden, intensief aangewend. Een aanpassing van de beveiliging door het slachtoffer zal daarom na een geslaagde inbraak in ieder geval zijn aangewezen. In rechte is slechts summiere informatie over het beveiligingssysteem vereist, om in dit opzicht tot een veroordeling te kunnen komen."

49. Deze passage is om twee redenen van belang. De eerste is dat daaruit blijkt dat de ontwerpwetgever "een systeem van autorisatie" in beginsel als een reële beveiliging beschouwde. Dat betekent dat het onbevoegd gebruik van het juiste wachtwoord in beginsel als het binnendringen in een daartegen beveiligd werk moest worden aangemerkt. In zoverre bevestigt de MvT de hiervoor gegeven interpretatie van het commissievoorstel.

50. De tweede reden is dat het gestelde de gerezen bezwaren eerder zal hebben gevoed dan weggenomen. Het onbevoegd gebruik van het juiste wachtwoord lijkt immers niet steeds tot strafbaarheid te leiden. Als een hacker het wachtwoord heeft weten te achterhalen, moet de rechthebbende er rekening mee houden dat dit

wachtwoord in brede kring bekend wordt. Past hij desondanks het wachtwoord niet aan, dan is, zo lijkt in de weergegeven passage gelezen te moeten worden, niet alleen geen sprake van een adequate beveiliging, maar ook niet van de vereiste minimale beveiliging. Dat is een benadering die afwijkt van hetgeen met betrekking tot inbraak (art. 311 Sr) en huisvredebreuk (art. 138 Sr) geldend recht is. De inbreker kan niet zijn eigen straffeloosheid creëren door kopieën van de huissleutel die hij heeft bemachtigd in brede kring te verspreiden en daarvan kond te doen aan de bewoner. Natuurlijk doet die bewoner er verstandig aan om zijn huis van nieuwe sloten te voorzien, maar als hij dat nalaat, is nog steeds sprake van het gebruik van een valse sleutel als met behulp van een (kopie van) de weggenomen huissleutel wordt binnengetreden.

51. Meer in het algemeen lijkt de Minister van de rechthebbende te verlangen dat hij gelijke tred houdt met de ontwikkelingen in "de elektronische oorlogsvoering". Hoe geavanceerder en geniepiger de methoden van de hackers zijn, zo lijkt de gedachte te zijn, hoe hoger de eisen zijn waaraan de beveiliging moet voldoen wil de rechthebbende aanspraak hebben op de bescherming van de strafwet. Daarmee dreigde zich te realiseren waarvoor de critici beducht waren: de schuld wordt bij de rechthebbende gelegd. Als die zich onvoldoende heeft bewapend in de "oorlog" die tegen hem wordt gevoerd, zijn de "aanvallen" die onbevoegden op zijn geautomatiseerde systeem uitvoeren, straffeloos. Zo legitimeren de geniepige methoden zichzelf: zodra die methoden in zwang zijn, kunnen ze straffeloos worden gebruikt omdat de computerbezitter zich daar maar tegen moet beveiligen.

52. Het wekt zogezien geen verbazing dat de kritiek op het wetsvoorstel aanhield. Dit keer sorteerde die kritiek wel effect. De MvA ging vergezeld van een Nota van wijziging, die art. 138a van een nieuwe redactie voorzag.(21) Het voorgestelde artikel kwam daardoor als volgt te luiden:
" Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt gestraft hij die wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij
a. daarbij enige beveiliging doorbreekt of
b. de toegang verwerft door middel van listige kunstgrepen, een valse sleutel of door het aannemen van een valse hoedanigheid."

Volgens de MvA werd door deze redactiewijziging aan een aantal van de geuite bezwaren tegemoet gekomen.(22) Gesproken werd van een strafbaarstelling in "afgezwakte vorm", van een "nog soepeler regime" met betrekking tot de beveiligingseis.(23) De Minister nam daarbij met zoveel woorden afstand van hetgeen in de MvT was gesteld:(24)
"Ik neem hiermee afstand van de uitlatingen in de memorie van toelichting dat het moet gaan om een reële beveiliging en van de daaraan verbonden beschouwingen over het dynamische karakter van de beveiliging, althans wat betreft de strafrechtelijke relevantie daarvan. Ik hoop hiermee aan de verschillende naar voren gebrachte bezwaren tegemoet te zijn gekomen. "

53. De vraag is welke versoepeling met de redactiewijziging werd beoogd. Volgens de MvA is het nodig dat er "enige beveiliging" is, omdat "het doorbreken van die beveiliging het strafbare feit vormt". Er moet in rechte worden vastgesteld dat er "iets" is doorbroken. "Was er niets, dan kan er ook niets doorbroken zijn geweest."(25) Alleen in zoverre wordt aan de beveiligingseis vastgehouden. De versoepeling zit hierin dat "iets" aan beveiliging al voldoende is. Thans wordt voorgesteld, zo schrijft de Minister op p. 12, gegevens in geautomatiseerde bestanden te beschermen "door het doorbreken van veiligheidsmaatregelen strafbaar te stellen, zonder dat daarmee eisen worden gesteld aan de aard van de veiligheidsmaatregelen". Elders wordt gesteld dat "de onbelemmerde kennisneming" van gegevens die niet voor de betrokkene zijn bestemd, niet strafbaar is. "Strafbaarheid ontstaat eerst daar waar doelbewust getroffen voorzieningen met het oog op geheimhouding worden omzeild, om aldus de kennelijk door de rechthebbende niet gewenste kennisneming van gegevens toch te bewerkstelligen."(26) Niet méér vereist is dus dan dat de wil van de betrokkene kenbaar is uit getroffen beveiligingsmaatregelen.(27) Uitdrukkelijk wordt gesteld dat het onbevoegd gebruikmaken van een wachtwoord steeds strafbaar binnendringen oplevert (p. 31, 32). Dat geldt ook als de kraker het password door onachtzaamheid van de rechthebbende heeft verkregen (p. 29). Dat geldt zelfs als de beheerder na een succesvolle inbraak zijn passwords niet zou wijzigen "hoewel deze op een bulletinboard voor een ieder bereikbaar zijn" (p. 31). Nalatigheid van de beheerder om de beveiliging aan te passen, leidt daarom niet tot straffeloosheid van de kraker (p. 32).

54. De vraag is of de gewijzigde redactie tot uitdrukking brengt wat gezien de in de MvA gegeven toelichting kennelijk de bedoeling was. Als winst ten opzichte van de oorspronkelijke redactie kan worden beschouwd dat er geen misverstand over kan bestaan dat het gebruik van een valse sleutel of een valse hoedanigheid tot strafbaarheid leidt. Een aanvullende beveiligingseis wordt niet gesteld. Maar tegelijk wordt nieuw leven geblazen in het oude misverstand dat het gebruik van een valse sleutel nog niet betekent dat wordt binnengedrongen in een daartegen beveiligde computer. Tekstueel gezien is het gebruik van een valse sleutel immers iets anders dan het doorbreken van een beveiliging. De redactie nodigt daardoor als het ware uit tot de gedachte dat het gebruik van een valse sleutel - en hetzelfde geldt voor de andere onder b. opgesomde methoden - weliswaar strafbaar is, maar dat dit zo is ondanks het feit dat er geen beveiliging is doorbroken. Het is dan nog maar een klein stapje naar de gedachte dat een geautomatiseerd werk dat 'slechts' voorzien is van een systeem van autorisatie geen beveiligde computer is.

55. Deze letterlijke interpretatie strookt niet met wat in de MvA wordt gesteld. Het strafbare feit van art. 138a Sr bestaat volgens de Minister immers uit het doorbreken van beveiliging(smaatregelen). Dat kan moeilijk anders begrepen worden dan dat ook het gebruik van de onder b. opgesomde methoden een doorbreking van de beveiliging oplevert. En dat impliceert dat een systeem van autorisatie het vereiste "iets"

aan beveiliging is dat doorbroken wordt als bijvoorbeeld een valse sleutel wordt gehanteerd. Dit vindt bevestiging in de toelichting op de gewijzigde redactie die in de Nota van wijziging wordt gegeven:(28)
" Artikel 138a stelt in zijn nieuw voorgestelde vorm strafbaar elke vorm van binnendringen, zowel wanneer daartoe een beveiliging is doorbroken, als wanneer een valse sleutel, bij voorbeeld een password, een valse hoedanigheid of listige kunstgrepen zijn aangewend. De straffeloosheid wordt daardoor beperkt tot de gevallen dat geen enkele beveiliging op een geautomatiseerd werk is aangebracht."

Zo mogelijk nog duidelijker is wat de Minister stelt in de MvA aan de Eerste Kamer:(29)
" De leden van de PvdA-fractie vroegen zich verder af waarom in artikel 138a van het Wetboek van Strafrecht in het eerste lid, naast de doorbreking van beveiliging, in het onderdeel b nog enige handelingen expressis verbis zijn toegevoegd, die toch ook kunnen worden beschouwd als methoden om de beveiliging te doorbreken. Ik wijs erop dat in het oorspronkelijk wetsvoorstel werd volstaan met de eenvoudige doorbrekingseis. Met name van de kant van het bedrijfsleven is hiertegen bezwaar ingebracht. Men vreesde dat gegevens in geautomatiseerde werken daardoor onvoldoende zouden worden beschermd. Men was niet zeker dat in de jurisprudentie de bedoeling van de wetgever om slechts een laagdrempelige beveiligingseis toereikend te achten voor strafbaarheid van de inbreker, in alle gevallen zou worden gevolgd. Teneinde tegemoet te komen aan deze kritiek, zijn in het tweede onderdeel van het eerste lid van dit artikel, alsnog enige methoden opgesomd - het betreft inderdaad geen uitputtende opsomming - om de bedoeling van de wetgever duidelijker tot uitdrukking te brengen."

In dit antwoord wordt de wetsgeschiedenis wat vertekend, maar dat neemt niet weg dat wordt bevestigd dat het in onderdeel b van het voorgestelde art. 138 lid1 gaat om een (niet limitatieve) opsomming van methoden om enige beveiliging te doorbreken. Die opsomming was daarbij wenselijk (niet noodzakelijk) om de bedoeling van de wetgever met betrekking tot de beveiligingseis duidelijk te maken.(30)

56. De conclusie moet mijns inziens dan ook zijn dat het ook bij art. 138a lid 1 sub b (oud) Sr gaat om het doorbreken van enige beveiliging. Het gebruik van een valse sleutel vormt dus een species van het genus doorbreking van enige beveiliging. Gelet daarop is de redactie weinig gelukkig. Beter was het geweest als de niet limitatieve opsomming van methoden voorop was gesteld (in onderdeel a.) en als onderdeel b. vervolgens had geluid: "op andere wijze enige beveiliging doorbreekt".

57. De gegeven opsomming is, zei de Minister, niet limitatief. Op de vraag welke andere methoden er zijn om enige beveiliging te doorbreken, zoekt men in de wetsgeschiedenis tevergeefs naar een antwoord. Voorbeelden van een doorbreking van enige beveiliging die niet door de gegeven opsomming van methoden wordt gedekt, worden niet gegeven. Daarbij moet bedacht worden dat het antwoord dat de Minister de Eerste Kamer gaf, betrekking had op het voorgestelde art. 138a zoals dat was komen te luiden na de wijzigingen die daarin bij de Tweede nota van wijziging waren aangebracht. Wat eerst het gehele art. 138a was, werd nu art. 138a, eerste lid. Dat eerste lid kwam als volgt te luiden:
"Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij
a. daarbij enige beveiliging doorbreekt of
b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid."

De in onderdeel b. gegeven opsomming is in vergelijking met die in de eerdere redactie (zie punt 52) gewijzigd. De listige kunstgrepen zijn verdwenen, de technische ingreep en de valse signalen zijn toegevoegd. Op het hoe en waarom van deze wijziging wordt aanstonds ingegaan. Hier is van belang om te constateren dat de gegeven opsomming veel omvattender is geworden. Daardoor is de vraag of de meerwaarde van onderdeel a. die van een zekerheidshalve aangebracht vangnet overtreft.

58. In dit verband zij het volgende opgemerkt. De term 'doorbreking' van enige beveiliging roept associaties op met fysiek ingrijpen. Denkbaar is dat de rechthebbende zijn stand alone-computer beveiligt door die computer te plaatsen in een vertrek dat afgesloten is met een van een hangslot voorziene deur. Het intrappen van die deur zou dan wellicht als het doorbreken van enige beveiliging kunnen worden aangemerkt, al is het de vraag of de wetgever daarop het oog had. Om fysiek ingrijpen in de computer zelf (in de hardware) kan het echter in onderdeel a. niet gaan. Iedere poging om met behulp van de schroevedraaier, de nijptang en de soldeerbout tot de opgeslagen gegevens door te dringen, zal die gegevens alleen maar minder bereikbaar maken. Daarbij laat ik nog daar dat de hacker die gebruikmaakt van telecommunicatie, geeneens tot fysiek ingrijpen in staat is. Om het veranderen van de programmagegevens die voor de beveiliging zorg dragen, kan het in onderdeel a. evenmin gaan. Want om die gegevens te kunnen veranderen, moet men eerst toegang tot die gegevens hebben. De vraag is hoe die toegang wordt verkregen.

59. Als ik het wel heb, is de enige manier om toegang te krijgen tot gegevens die in een geautomatiseerd zijn opgeslagen, het verzenden van signalen waarop dat geautomatiseerde werk reageert. En dat kan alleen als dat geautomatiseerde werk zodanig is geprogrammeerd, dat op die signalen wordt gereageerd. Dat betekent dat de toegang tot een geautomatiseerd werk alleen kan worden verkregen door gebruikmaking van de programmatische mogelijkheden van de desbetreffende computer. Dat geldt ook voor de hacker. Blijkens zijn ter terechtzitting van het Hof overgelegde pleitnota (p. 7) heeft de raadsman van de verdachte aldaar de volgende kritiek geleverd op het aanvullende proces-verbaal van verbalisant [verbalisant 1] (door het Hof gebezigd als bewijsmiddel 17; zie ook bewijsoverweging D2 onder r.):
"[verbalisant 1] stelt in de vierde alinea: "Het kenmerk van deze nieuwe methoden is dat ze door middel van

het opzettelijk geven van verkeerde signalen aan delen van het Windows besturingssysteem, dit systeem dusdanig in de war kunnen brengen, dat deze delen tijdelijk onbruikbaar raken en zelfs crashen." Dat is onjuist.
Als je een protocol, in het geval van [verbalisant 1] het RPC protocol, niet middels correcte headers (afgesproken signalen) benaderd, zal deze het verkeer/verbinding niet herkennen en het verkeer totaal negeren. Het hanteren van een vals signaal heeft dus geen enkel effect. Vergelijk het met het huis van de buren trachten binnen te komen, met gebruik van je eigen voordeelsleutel. Dat werkt niet."

Uit het verweer spreekt de beroepstrots van de ware hacker. Natuurlijk is het Toxbot niet zo geprogammeerd dat het verkeerde signalen afgeeft. De kunst is juist om de goede signalen af te geven, de signalen waarop het geautomatiseerde systeem is (voor)geprogrammeerd. Alleen zo kan men tot dat systeem doordringen. De hacker maakt dus per definitie gebruik van de wijze waarop het systeem is geprogrammeerd. In die zin wordt er niets "doorbroken". Het systeem (de wijze waarop het is geprogrammeerd) blijft geheel in tact. Juist daardoor kan ervan worden geprofiteerd.

60. Uit het voorgaande volgt niet dat de kritiek van de raadsman hout snijdt. Veeleer volgt daaruit dat die kritiek nergens op slaat. Het begrip 'doorbreken van enige beveiliging' kan door de wetgever niet anders dan in overdrachtelijke zin zijn gebezigd. Op het onmogelijke kan de wetgever immers niet het oog hebben gehad. Het kan niet zo zijn dat de aanwezige beveiliging (dat wil zeggen de programma's die daarvoor zorgen) op een of andere manier geweld moet zijn aangedaan. Wat strafbaar is gesteld, is het geven van in technisch opzicht correcte signalen (dat wil zeggen signalen die door het systeem worden herkend en waarop het systeem conform zijn programmering respondeert). De vraag waarop het aankomt, is wanneer het geven van dergelijke correcte signalen als het doorbreken van een beveiliging in de zin van art. 138a Sr moet worden aangemerkt. Onderdeel b. van art. 138a lid 1 (oud) Sr geeft op die vraag in elk geval een begin van een antwoord. Daarom zal nu eerst een antwoord worden gezocht op de vraag op welke methoden de wetgever met de gegeven opsomming het oog heeft gehad.

61. In het rapport van de Commissie Franken - waarop het oorspronkelijke wetsvoorstel was gebaseerd - wordt met betrekking tot de begrippen 'valse hoedanigheid', 'listige kunstgrepen' en 'valse sleutel' opgemerkt dat daarmee beoogd wordt "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 toegangsmiddelen".(31) De term 'listige kunstgrepen' zou daarbij zien op de ingenieuze manieren die hackers hanteren om achter de toegangscodes te komen. Die term paste niet goed in het rijtje, omdat het niet gaat om een (geldig) toegangsmiddel, maar om de manier waarop dat middel wordt verkregen. En die doet niet ter zake (zie punt 53).(32) Of dat de reden is dat de listige kunstgrepen als manier om de beveiliging te doorbreken bij de Tweede nota van wijziging afvielen, is overigens de vraag. Vergelijk hierna, punt 67. De termen 'valse hoedanigheid' en 'valse sleutel' zagen volgens de Commissie wél op het gebruik dat van het (niet legaal verkregen) toegangsmiddel werd gemaakt. Als voorbeelden van beide termen noemt de Commissie de magneetpas en de toegangscode (als zij zonder toestemming worden gebruikt). Het verschil zou daarbij zitten in de toegangsprocedure. Van het gebruik van een valse sleutel was sprake "wanneer de toegangsprocedure niet in een identificatie doch slechts in een autorisatie van de gebruiker voorziet". Anders zou sprake zijn van het gebruik van een valse hoedanigheid. Men kan vraagtekens plaatsen bij de houdbaarheid, de hanteerbaarheid en de relevantie van dit onderscheid. Ik merk slechts op dat het onbevoegd gebruik van een password in de MvA consequent als het gebruik van een valse sleutel wordt bestempeld, hoewel dat alleen juist zou zijn als de autorisatieprocedure niet in identificatie zou voorzien. En dat lijkt zelden of nooit het geval te zijn.(33)

62. Uit het voorgaande kunnen twee conclusies worden getrokken. De eerste is dat het onderscheid tussen het gebruik van een valse hoedanigheid en het gebruik van een valse sleutel niet helder is. Erg is dat niet omdat aan het onderscheid geen rechtsgevolgen zijn verbonden. Het gebruik van beide toegangsmiddelen is strafbaar. De tweede conclusie is dat beide toegangsmiddelen betrekking hebben op de normale toegangsprocedure die ook door de rechthebbende wordt doorlopen. De hacker die deze middelen hanteert gebruikt dezelfde ingang als de rechthebbende en verzendt daarbij dezelfde signalen. Het verschil is alleen dat de hacker niet bevoegd is deze signalen te verzenden.

63. De 'technische ingreep' en de 'valse signalen' zijn als gezegd bij de Tweede nota van wijziging in het voorgestelde eerste lid van art. 138a terechtgekomen. Deze toevoeging hield verband met de stapsgewijze introductie in het wetsvoorstel van art. 326c Sr, waarin beide termen eveneens voorkomen.(34) Het artikel verving art. 50 lid 3 van de (inmiddels vervallen) Wet op de telecommunicatievoorzieningen. Dit artikellid luidde als volgt:
" Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, door een technische ingreep het verrichten van een dienst met gebruikmaking van de telecommunicatie infrastructuur of een draadomroepinrichting als bedoeld in artikel 21 bewerkstelligt, wordt gestraft met gevangenisstraf van ten hoogste vier jaar of geldboete van de vijfde categorie."

De MvT op deze strafbepaling vermeldde dat daarmee werd voorzien in een leemte die door de Commissie Franken was gesignaleerd.(35) Overheveling van de bepaling naar het Wetboek van Strafrecht werd daarbij in het vooruitzicht gesteld. Met betrekking tot het begrip 'technische ingreep' wordt het volgende opgemerkt:
"Onder "technische ingreep" wordt verstaan elke vorm van technische manipulatie, zowel van buitenaf als in de telecommunicatie-infrastructuur en de draadomroepinrichting, die leidt tot het verrichten van de hierbedoelde diensten. Ook waar dit gevolg wordt bereikt louter ten gevolge van een door een technische ingreep rechtstreeks inwerking stellen van een mechanisme."

In het bijzonder de laatste zin lijkt erop te duiden dat bij een 'technische ingreep' ook en misschien wel vooral werd gedacht aan fysiek ingrijpen in de telecommunicatie-infrastructuur. Ook de toevoeging van de 'valse signalen' in het voorgestelde art. 326c lijkt daarop te wijzen. In de Nota van wijziging wordt daarover het volgende gesteld:(36)
" Bij de totstandkoming van de Wet op de telecommunicatievoorzieningen is voorzien in een strafbaarstelling van een vorm van bedrog door middel van de telecommunicatie-infrastructuur. Daar het hier gaat om een naar verhouding ernstig misdrijf, dat samenhang vertoont met andere bedrogsbepalingen in het Wetboek van Strafrecht, is het wenselijk deze strafbepaling als een nieuw artikel 326c op te nemen in het Wetboek van Strafrecht. Tegelijkertijd is de bepalmg op een onderdeel aangevuld met het bestanddeel "met behulp van valse signalen". In de praktijk blijken lieden er in te zijn geslaagd door het uitzenden van bepaalde signalen de telefooncentrale die deel uitmaakt van de telecommunicatie-infrastructuur, te misleiden in die zin dat zij daardoor zonder te betalen of ten laste van een niets vermoedende derde, gebruik kunnen maken van via de telecommunicatie-infrastructuur aangeboden diensten. Dergelijke signalen kunnen bezwaarlijk worden begrepen als "een technische ingreep" in de zin van het bestaande artikel 50, derde lid, van de Wet op de telecommunicatievoorzieningen. De strekking van de bepaling blijft ongewijzigd.
Het begrip "valse signalen" komt al voor in artikel 142 van het Wetboek van Strafrecht. Het betekent in het algemeen dat enig teken wordt gegeven dat bij de ontvanger, ongeacht of dit een natuurlijke persoon of een geautomatiseerd werk is, een gevolg bewerkstelligt dat gebaseerd is op (geprogrammeerde) veronderstellingen die onjuist blijken te zijn, terwijl degeen die het teken geeft, weet dat hij met dat teken, gegeven die veronderstellingen, dat gevolg uitlokt. De ontvanger wordt dus misleid: indien het gaat om een natuurlijke persoon in letterlijke zin, indien het gaat om een geautomatiseerd werk in overdrachtelijke zin. Ik verwijs verder naar de jurisprudentie omtrent het begrip "valse" in de uitdrukking "valse sleutels" in de artikelen 90 en 138, tweede lid, met name het arrest van 20 mei 1986 (NJ 1987, 130) waarbij is vastgesteld dat het gebruik van een huissleutel die tot opening van het slot van de toegangsdeur van een woning wordt gebruikt door iemand die daaroe geen recht heeft, ten aanzien van dat slot een valse sleutel is.
Onder onderdeel XI van de nota van wijziging wordt voorgesteld het desbetreffende artikellid van de Wet op de telecommunicatievoorzieningen te laten vervallen."

In de Tweede nota van wijziging werd een verzwaarde vorm van computervredebreuk strafbaar gesteld, neergelegd in het nieuwe tweede (later derde) lid van art. 138a. Er werd op gewezen dat het bedoelde computermisbruik maar ten dele door het voorgestelde art. 326c werd gedekt en dat, om tot een betere afbakening te komen, ook art. 326c moest worden gepreciseerd.(37) De gesignaleerde verwantschap tussen beide strafbaarstellingen is kennelijk de reden geweest dat de 'technische ingreep' en de 'valse signalen' werden opgenomen in de in onderdeel b. van het eerste lid van art. 138a.

64. Men kan zich afvragen of de wetgever aan dat laatste goed heeft gedaan. De bedoelde begrippen hebben in het kader van art. 326c Sr nog wel een enigszins te omlijnen inhoud doordat zij verwijzen naar concrete vormen van misbruik van telecommunicatie die de wetgever wenste tegen te gaan. De overplanting van deze begrippen naar art. 138a maakt dat anders. In het kader van dat artikel is het niet eenvoudig zich een concrete voorstelling te maken van hetgeen bedoeld zou kunnen zijn. De toch al wazige formuleringen waarmee deze begrippen werden toegelicht, lijken hier alle betekenis te verliezen. Het onderscheid tusen beide begrippen kan in het kader van art. 138a in elk geval niet meer gezocht worden in de vraag of louter (valse) signalen zijn verzonden, dan wel of er iets is veranderd door fysiek ingrijpen of door het wijzigingen van programmagegevens. Programmagegevens kan men immers pas veranderen als reeds toegang tot het geautomatiseerde werk is verkregen. En door fysiek ingrijpen (zoals het doorknippen en anders verbinden van kabels) verkrijgt men geen toegang tot een geautomatiseerd werk. Daarvoor is nodig dat (al dan niet door tussenkomst van gemanipuleerde kabels) signalen worden verzonden waarop dat werk reageert conform zijn "(geprogrammeerde) veronderstellingen". Een 'technische ingreep' waardoor toegang tot een geautomatiseerd werk wordt verkregen, kan anders gezegd moeilijk anders worden gerealiseerd dan door middel van 'valse signalen'.

65. Niet alleen is onduidelijk wat in een digitale context precies het verschil is tussen de technische ingreep en het gebruik van valse signalen, onhelder is ook hoe het gebruik van die valse signalen zich verhoudt tot het gebruik van een valse hoedanigheid of een valse sleutel. In de Nota van wijziging wordt zoals wij zagen gesteld dat de ontvanger door de valse signalen wordt misleid. In technische zin echter kan een computer niet worden 'misleid' door 'verkeerde' signalen. De computer reageert zoals hij is geprogrammeerd. Van "(geprogrammeerde) veronderstellingen die onjuist blijken te zijn" kan dan ook alleen in overdrachtelijke zin worden gesproken. Bedoeld zijn mogelijk de veronderstellingen die de programmeurs hadden en de rechthebbenden koesteren over het gebruik dat van de geprogrammeerde mogelijkheden wordt gemaakt. Van onbehoorlijk gebruik, gebruik waarvoor zij het systeem niet hebben ontworpen of bestemd, zijn zij niet uitgegaan. Welnu, ingeval van het gebruik van een valse sleutel of een valse hoedanigheid kan gesproken worden van het verzenden van signalen die niet overeenkomen met de "geprogrammeerde veronderstelling" dat alleen een bevoegde van het password gebruik zal maken. In de Nota van wijziging wordt, zoals wij zagen, uitdrukkelijk verwezen naar de jurisprudentie omtrent het begrip valse sleutel in de artikelen 90 en 138 Sr. De conclusie lijkt voor de hand te liggen dat het gebruik van een valse sleutel of een valse hoedanigheid een subcategorie van het gebruik van valse signalen is.

66. Een verschil tussen de valse sleutel en de valse hoedanigheid enerzijds en de technische ingreep en de valse signalen anderzijds is dat het bij de eerste twee toegangsmiddelen steeds gaat om gebruikmaking van de normale ingang tot het geautomiseerde werk, terwijl dit bij de laatste twee niet per se het geval behoeft te zijn. Ook trucs die erop gericht zijn andere, 'abnormale' ingangen te benutten, zouden daaronder kunnen

worden gebracht. Een argument voor een dergelijke ruime uitleg kan ontleend worden aan het feit dat de laatste twee begrippen ontleend zijn aan art. 326c. In de Nota naar aanleiding van het Eindverslag (TK 1991-1992, 21551, nr 11, p. 23) wordt de suggestie van de vaste Commissie voor Justitie om in het voorgestelde art. 326c de term 'listige kunstgrepen' te hanteren in plaats van de technische ingreep en de valse signalen als volgt gepareerd:
" Ik deel het oordeel van de Commissie niet. Met de term "listige kunstgrepen" in het bestaande artikel 326 heeft de wetgever indertijd de beperking willen aanbrengen dat niet strafbaar is de situatie waarbij het slachtoffer zich met open ogen laat bedriegen. Er moet iets "listigs" aan de kunstgrepen zijn, zodat het slachtoffer er niet op bedacht had hoeven zijn dat hij werd bedrogen. Daardoor ontstaat ook pas een zodanige verwijtbaarheid aan de kant van de dader, dat van strafwaardig gedrag kan worden gesproken. Dergelijke overwegingen passen niet in een geautomatiseerde omgeving. Uiterst eenvoudige technische ingrepen of valse signalen waaraan geen listig aspect valt te bekennen, kunnen worden aangewend om diensten te verwerven die met behulp van telecommunicatie worden aangeboden. Ik acht het van belang dat al dergelijke vormen van bedrieglijkheden met behulp van informatietechniek worden gedekt, zonder dat in rechte behoeft te worden vastgesteld of het geautomatiseerd werk dat met dergelijke signalen of technische ingrepen wordt geconfronteerd, dergelijke trucs eenvoudig had moeten "doorzien"."

De Minister wenste alle vormen van bedrieglijkheden met behulp van informatietechniek te dekken met de begrippen technische ingreep en valse signalen. Dat roept de vraag op of die begrippen in het kader van art. 138a ook niet alle bedrieglijkheden dekken. Zijn er manieren om de beveiliging te doorbreken die niet bestaan uit een technische ingreep of het gebruik van valse signalen?

67. Wij zagen dat de term 'listige kunstgrepen' aanvankelijk ook in het voorgestelde art. 138a voorkwam. De zojuist aangehaalde passage uit de Nota naar aanleiding van het Eindverslag verklaart mogelijk de vervanging van deze term door het begrippenpaar technische ingreep en valse signalen. De term zou te beperkt zijn omdat ook de toepassing van eenvoudige trucs tot strafbaarheid op grond van art. 138a zou moeten leiden. Dat past bij de afzwakking van de beveiligingseis die in de MvA haar beslag kreeg. Deze verklaring betekent intussen dat, als zij juist is, de Minister ongemerkt aan de term 'listige kunstgrepen' een andere inhoud is gaan geven dan die term in het door de regering overgenomen voorstel van de Commissie Franken had (zie hiervoor, punt 61).

68. De conclusie uit het voorgaande kan zijn dat de toevoeging van de technische ingreep en de valse signalen aan de in onderdeel b. opgenomen toegangsmiddelen weinig doordacht is geweest. De vier opgesomde toegangsmiddelen hebben een onzekere inhoud, hetgeen wordt geïllustreerd door het feit dat de door de Commissie Franken geïntroduceerde toegangsmiddelen in de loop van het wetgevingsproces van kleur zijn verschoten. Aan het verschil dat de Commissie zag tussen de valse sleutel en de valse hoedanigheid lijkt niet te zijn vastgehouden. Meer in het algemeen geldt dat een onderlinge afbakening van de opgesomde toegangsmiddelen niet wel mogelijk is. De begrippen lijken elkaar goeddeels te overlappen en zelfs geheel in elkaar op te gaan. De begrippen kunnen daarbij mede vanwege hun vaagheid zo ruim worden uitgelegd, dat zij alle vormen van doorbreking van de beveiliging dekken. De functie die de opsomming van toegangsmiddelen aanvankelijk had - namelijk zeker stellen dat het onbevoegd gebruik van toegangscodes strafbaar was - is daardoor verloren gegaan. Alle trucs - de listige en de kinderlijk eenvoudige - kunnen in onderdeel b een plaats vinden.

69. Deze conclusie vindt tot op zekere hoogte bevestiging in de wordingsgeschiedenis van de - na het plegen van de onderhavige feiten in werking getreden - Wet computercriminaliteit II. In de Tweede Nota van wijziging wordt toegelicht wat onder een 'technische ingreep' als bedoeld in art. 138a Sr moet worden verstaan.(38) Dit omdat deze term destijds zonder nadere toelichting zou zijn geïntroduceerd. Uiteengezet wordt dat de term is ontleend aan art. 50 lid 3 Wet op de telecommunicatievoorziening (dat de basis vormde voor art. 326c Sr) en dat het daarbij gaat om een "specifiek op telecommunicatie toegespitste vorm van oplichting". Op grond daarvan wordt geconcludeerd dat de 'technische ingreep' een "vertaling [was] van de oplichtingsmiddelen naar de technische omgeving van de telecommunicatie". Vervolgens wordt gesteld:
" Toegespitst op artikel 138a betekent dit het volgende. Het verwerven van toegang tot een geautomatiseerd werkdoor een technische ingreep veronderstelt een ingreep in c.q. het manipuleren van het technisch functioneren van het geautomatiseerde werk. Het louter intoetsen van een (al of niet vals) wachtwoord zal aldus niet als een technische ingreep kunnen worden beschouwd, omdat de afhandeling daarvan de functionaliteit van het systeem intact laat. Maar het intoetsen van een combinatie van tekens die als doel heeft het technisch functioneren van het geautomatiseerde werk zodanig te veranderen dat, ondanks het ontbreken van het juiste wachtwoord, toegang verworven kan worden, kan onder omstandigheden wel als technische ingreep worden beschouwd. In een dergelijk geval zal ook sprake kunnen zijn van het doorbreken van een beveiliging en/of van het gebruikvan valse signalen of een "valse sleutel". Een nauw omlijnde interpretatie van deze begrippen is echter, zeker in de nieuwe opzet van artikel 138a, van beperkte betekenis, aangezien de rechter de vrijheid wordt gelaten om ookin andere gevallen vast te stellen dat sprake is van "binnendringen" in de zin van die bepaling."

Een "nauw omlijnde interpretatie" kan, zo mag geconcludeerd worden, niet gegeven worden. Een en dezelfde truc kan onder verschillende begrippen tegelijk vallen. Ook van een scherpe scheiding tussen de onderdelen a. en b. van art. 138a lid 1 (oud) Sr is geen sprake. Een technische ingreep kan ook het doorbreken van een beveiliging opleveren.

70. In de zojuist aangehaalde passage wordt gesteld dat een nauw omlijnde interpretatie in de nieuwe opzet van art. 138a van beperkte betekenis is. Die nieuwe opzet, of beter: de reden die daaraan ten grondslag ligt,

kan hier niet onbesproken blijven. Het eerste lid van art. 138a in de gewijzigde opzet is als volgt komen te luiden:
"1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie 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."

Volgens de Minister was de nieuw gekozen opzet noodzakelijk om tegemoet te komen aan de eisen die in het bijzonder voortvloeiden uit het Kaderbesluit 2005/222/JBZ van 24 februari 2005 over aanvallen op informatiesystemen (PbL 2005/69, p. 67).(39) Dit Kaderbesluit verplicht tot de strafbaarstelling van hacken. Volgens art. 2 lid 2 van dat Kaderbesluit kan iedere lidstaat de strafbaarstelling afhankelijk maken van een inbreuk op beveiligingsmaatregelen. Van andere voorwaarden, zo redeneerde de Minister, dus niet. Daaruit zou volgen dat art. 138a Sr zoals dat toen luidde, niet met het Kaderbesluit in overeenstemming was. Want daarin werd de strafbaarheid niet alleen afhankelijk gemaakt van de doorbreking van een beveiliging, maar ook van de in onderdeel b. opgesomde methoden. Op deze argumentatie is heel wat af te dingen. De belangrijkste tegenwerping is dat de stelling dat het bij onderdeel b. niet gaat om beveiligingsmaatregelen, lijkt te getuigen van een misvatting.(40) Die stelling is zelfs moeilijk te rijmen met hetgeen bij gelegenheid van dezelfde wetgevingsoperatie werd gesteld met betrekking tot het begrip 'technische ingreep'. Volgens de Tweede nota van wijziging kan een technische ingreep immers ook een doorbreking van enige beveiliging zijn.

71. Of aan de argumentatie van de Minister betekenis toekomt als het om de uitleg van het huidige art. 138a Sr gaat, kan hier in het midden blijven. Een authentieke interpretatie van het toen geldende recht levert zij in elk geval niet op. Ik meen dan ook dat daaraan hier voorbijgegaan mag worden.

72. Volgens de Minister is een nauw omlijnde interpretatie "zeker" in de nieuwe opzet van art. 138a van beperkte betekenis. De vraag is of niet hetzelfde geldt voor de oude opzet van het artikel. Als de wetgever er niet in slaagt om een helder omlijnd begrippenapparaat te presenteren, mag van de rechter niet verwacht worden dat hij er wél chocola van weet te maken.

73. Ik merk daarbij op dat de op art. 138a toegespitste verduidelijking die werd gegeven (hiervoor, punt 69), ons ook wat het oude recht betreft niet verder brengt. Wat men zich bij een verandering van het "technisch functioneren" van het geautomatiseerde werk moet voorstellen, blijft in nevelen gehuld. Om fysieke ingrepen in de hardware of om het veranderen van het besturingsprogramma kan het in het kader van art. 138a niet gaan. Toegang tot een geautomatiseerd systeem kan alleen worden verkregen door gebruikmaking van de mogelijkheden tot toegang die zijn ingeprogrammeerd. De hacker verandert het technisch functioneren van het systeem dus niet, hij maakt daar juist gebruik van. Daarin is mijns inziens tegelijk de verklaring gelegen voor het feit dat de verschillende toegangsmiddelen zich niet nauwkeurig laten omlijnen. De hacker maakt gebruik - of wellicht beter: misbruik - van de mogelijkheden die het systeem biedt. De gehanteerde methoden worden dus door die mogelijkheden bepaald. Dat betekent dat die methoden zich in technisch opzicht alleen laten onderscheiden door onderscheid te maken tussen de vele en uiteenlopende mogelijkheden die de verschillende systemen te bieden hebben. En dat is een hachelijke onderneming, zeker voor een wetgeving die techniek-onafhankelijk pretendeert te zijn.

74. Om de verschillen in technisch opzicht kan het bij de onderscheiden methoden dus niet, of slechts in beperkte mate gaan. Wij zagen dat het gebruik van een valse sleutel of een valse hoedanigheid technisch gezien kan worden gekoppeld aan de normale toegangsprocedure, aan het ingeprogrammeerde systeem van autorisatie. Maar het lijkt niet zo te zijn dat de beide andere methoden uitsluitend betrekking hebben op de 'abnormale' ingangen die het systeem te bieden heeft (vergelijk punt 66). Als die methoden betrekking hebben op alle geprogrammeerde toegangsmogelijkheden van het systeem, laten zij zich in technisch opzicht niet van elkaar onderscheiden. De retorische vraag is natuurlijk: waarin dan wel?

75. De vraag waarop het aankomt, zo stelde ik eerder (punt 60), is wanneer het geven van in technisch opzicht correcte signalen aan een geautomatiseerd systeem als het doorbreken van een beveiliging in de zin van art. 138a Sr moet worden aangemerkt. Het antwoord kan niet in de techniek gevonden worden. Dat betekent dat het antwoord normatief van aard is. Wat een password tot een valse sleutel maakt, is de onbevoegdheid van het gebruik. Daarin verschilt die methode niet van de andere methoden waarmee men zich de toegang tot een geautomatiseerd systeem kan verschaffen. Correcte signalen doorbreken de beveiliging als zij onbevoegd worden gegeven, als daardoor misbruik wordt gemaakt van de technische mogelijkheden die in het systeem zijn ingebakken. Daarbij is niet méér vereist dan dat op grond van enige daad van beveiliging objectief duidelijk is dat sprake is van misbruik, dat de 'correcte' signalen onbevoegd worden gegeven. Als de normale toegang tot bepaalde delen van de computer is beveiligd door een systeem van autorisatie, volgt daaruit dat het gebruiken van de andere toegangsmogelijkheden die het systeem kent, misbruik van die mogelijkheden oplevert, zeker als het gaat om willekeurige derden.

76. Ik roep in herinnering dat de wetgever alleen de onbelemmerde toegang straffeloos wilde laten (hiervoor, punt 53). Van een dergelijke onbelemmerde toegang is sprake bij de vele websites waar men op internet naar toe kan surfen. Van een onbelemmerde toegang is geen sprake als men stuit op schermen waarop

inlogcodes moeten worden ingevuld. Dat die schermen voor een hacker mogelijk geen barrière vormen, doet daaraan niet af. Hetzelfde geldt a fortioro als men in het geheel niet stuit op schermen die toegang tot het systeem verschaffen. Van een onbelemmerde toegang kan dan bezwaarlijk gesproken worden. Dat er hidden shares zijn, die het voor een hacker een koud kunstje maken om binnen te dringen, maakt dat niet anders. Adequaat behoeft de beveiliging immers niet te zijn.

77. Moeilijker moeten we het mijns inziens niet proberen te maken. Art. 138a Sr vraagt om een normatieve invulling die functioneel is, die voorziet in een effectieve strafrechtelijke bescherming tegen onbevoegde kennisneming van in geautomatiseerd werken opgeslagen gegevens. Het criterium voor de vraag of onbevoegd gebruik is gemaakt van de ingeprogrammeerde toegangsmogelijkheden van een geautomatiseerd systeem, zou ik dan ook, wat de toegang door middel van telecommunicatie betreft, willen zoeken in hetgeen in het maatschappelijk (internet)verkeer algemeen geaccepteerd is. Alle methoden van toegangverschaffing die het normale, algemeen geaccepteerde gebruik van de programmatische mogelijkheden van op de telecommunicatie-infrastructuur aangesloten systemen te buiten gaan, leveren in beginsel het onbevoegd gebruik van die mogelijkheden op.

78. Bij de hier geschetste stand van zaken is het mijns inziens niet nodig dat de rechter een keuze maakt uit de verschillende mogelijkheden van evident onbevoegd gebruik die in de onderdelen a. en b. van art. 138a lid 1 (oud) Sr worden genoemd. In veel gevallen is een dergelijke keuze niet doenlijk. En in geen enkel geval is een dergelijke keuze strafrechtelijk relevant. Daarom kan de in onderdeel b. gegeven opsomming maar het beste in haar geheel worden gezien als een poging om te verduidelijken wat onder het doorbreken van enige beveiliging moet worden verstaan. Zelfstandige betekenis komt aan die (weinig geslaagde) poging niet toe.

79. Na deze lang uitgevallen aanloop kan ik over het middel betrekkelijk kort zijn. Aangevoerd wordt dat het Hof, door in aanmerking te nemen dat een standaard Windows XP installatie is beveiligd tegen inloggen van buitenaf, een verkeerde maatstaf heeft aangelegd. Dit omdat de verdachte juist niet heeft ingelogd, maar de computer op andere wijze is binnengegaan. Die klacht berust op een onjuiste rechtsopvatting. Juist het feit dat de computer is beveiligd tegen inloggen van buitenaf, maakt dat het op andere wijze binnendringen van die computer als het doorbreken van een beveiliging moet worden aangemerkt.

80. De stelling dat de computers met Windows XP, servicepack 0, niet zijn beveiligd, berust dan ook op een onjuiste rechtsopvatting. Dat, zoals wordt betoogd, slechts gebruik gemaakt is van de "gaten in de beveiliging" impliceert dat er wel enige beveiliging was, hoe gebrekkig die beveiliging in de ogen van de verdachte wellicht ook was. De wetgever eist niet dat de rechthebbende gelijke tred houdt met de "voortdurende technologische oorlogsvoering". Dat servicepack 1 en 2 ontbreken, wil dus niet zeggen dat het boevenpak straffeloos zijn gang kan gaan.

81. De beeldende vergelijking die verweer en middel maken met het huis waarvan alle ramen en deuren openstaan, gaat dan ook mank. Als alle deuren en ramen openstaan, is het huis inderdaad op geen enkele wijze beveiligd. Maar als de deur (de normale toegang tot het huis) dicht zit en alle ramen staan open, is er wel enige beveiliging. De ongenode gast die door het raam naar binnengaat, maakt zich schuldig aan inklimming, hetgeen hem even zwaar wordt aangerekend als braak of verbreking. Zijn gedrag levert huisvredebreuk op (art. 138 lid 2). Dat men het huis gemakkelijk kan binnengaan (dat de beveiliging gebrekkig was), maakt vanuit normatief gezichtspunt dus geen verschil. Met computervredebreuk is het niet anders. Het middel lijkt op de opvatting te berusten dat iedere mogelijkheid om het systeem binnen te dringen, van een aparte, afdoende beveiliging moet zijn voorzien. Die opvatting brengt, consequent doorgedacht, mee dat hacking die niet bestaat uit het onbevoegd gebruik van toegangscodes, nooit strafbaar is. Want men kan alleen toegang krijgen tot een geautomatiseerd werk door gebruikmaking van de 'gaten' die in de programmatuur van dat werk besloten liggen. Zodra beveiligingsmaatregelen verhinderen dat van dat gat gebruik wordt gemaakt, biedt het geautomatiseerde systeem niet meer de mogelijkheid om langs die weg binnen te dringen. En omgekeerd: als op een bepaalde wijze is binnengedrongen, betekent dat dat het werk daartegen niet beveiligd was.

82. Het Hof heeft in het voetspoor van de tenlastelegging bewezenverklaard dat "verdachte en zijn medeverdachte de beveiliging hebben doorbroken, in elk geval de toegang hebben verworven door een technische ingreep, met behulp van valse signalen en/of door het aannemen van een valse hoedanigheid". Ik denk dat dit gelezen zou moeten worden als: dat "verdachte en zijn medeverdachte de toegang hebben verworven door een technische ingreep, met behulp van valse signalen en/of door het aannemen van een valse hoedanigheid, in elk geval de beveiliging hebben doorbroken" (vgl. punt 56). Maar wat daarvan ook zij, het Hof heeft op grond van hetgeen het heeft vastgesteld - namelijk dat de verdachte en zijn medeverdachte, hoewel de desbetreffende computers beveiligd waren tegen inloggen van buitenaf, desondanks van buitenaf die computers zijn binnengedrongen met behulp van een daartoe ontwikkeld wormvirus en aldus misbruik hebben gemaakt van de kwetsbaarheid van die systemen - met juistheid geoordeeld dat sprake was van het doorbreken van enige beveiliging en tevens dat, gelet op de niet vast omlijnde betekenis van die term, sprake was van een technische ingreep.

83. In de schriftuur wordt nog geklaagd over de begrijpelijkheid van 's Hofs oordeel dat sprake was van een technische ingreep omdat de verdachten "verhuld en onherkenbaar, middels het 'verpakte' virus" zijn binnengedrongen (zie punt 39; onder D4). Aangevoerd wordt dat uit de bewijsmiddelen blijkt de verpakking van het virus diende om herkenning door een virusscanner van het reeds binnengedrongen virus te voorkomen. Daaruit kan niet worden afgeleid dat de verpakking een rol speelde bij het doorbreken van de beveiliging. Hoewel die klacht mij terecht lijkt te zijn voorgedragen, kan zij niet tot cassatie leiden. Aan de

hiervoor bereikte slotsom doet het gestelde namelijk niet af.

84. Het Hof heeft tevens geoordeeld dat het bewezenverklaarde gebruik van een valse hoedanigheid hierin bestond dat de verdachte "gaten in systeembeveiliging opzocht ten einde als administrator/system [...] binnen te dringen". Als juist is dat het aannemen van een valse hoedanigheid alleen betrekking heeft op het onbevoegd gebruik van toegangscodes (vgl. punt 62), is dit oordeel van het Hof niet begrijpelijk. Het middel klaagt daarover echter niet.

85. Het middel faalt.

86. Beide middelen falen.

87. Ambtshalve vraag ik aandacht voor het volgende. Verdachte heeft op 26 september 2008 beroep in cassatie ingesteld. De Hoge Raad zal uitspraak doen nadat sedertdien meer dan vierentwintig maanden zijn verstreken. Dat brengt mee dat de redelijke termijn als bedoeld in artikel 6, eerste lid, EVRM is overschreden. Dat moet leiden tot strafvermindering.

88. Andere gronden waarop de Hoge Raad gebruik zou moeten maken van zijn bevoegdheid de bestreden uitspraak ambtshalve te vernietigen, heb ik niet aangetroffen.

89. Deze conclusie strekt tot vernietiging van het bestreden arrest voor wat betreft de opgelegde straf. De Hoge Raad kan de hoogte daarvan verminderen naar de gebruikelijke maatstaf. Voor het overige dient het beroep te worden verworpen.

De Procureur-Generaal
bij de Hoge Raad der Nederlanden

AG

1 Een botnet is een verzameling (netwerk) van computers (van derden) die - doorgaans via een (computer)worm, trojan of backdoor - met ongewenste software zijn geïnfecteerd en door die software worden gekoppeld. De beheerder van een botnet kan dit, doorgaans zonder dat gebruikers van de geïnfecteerde computers dit door hebben, op afstand besturen. Zie http://nl.wikipedia.org/wiki/Botnet. Vgl. pp. 7 en 14 van de Aanvulling bewijsmiddelen.
2 Zie onder meer bewijsmiddel 15 (p. 28).
3 Daarom kan het virus beschouwd worden als een worm, dat wil zeggen een virus dat zich zonder de tussenkomst van de gebruiker van de geïnfecteerde computer verder verspreidt. Vgl. bewijsmiddel 6 (p. 13).
4 Zie bewijsmiddel 8 (p. 14). Zie ook bewijsmiddel 11 (p. 24), waarin wordt gesteld: "Het botnet leek een grootte te hebben tussen de 50.000 en 80.000 computers. Tijdens de ontmanteling van het botnet bleken de aantallen veel hoger te liggen."
5 Een trojan (Trojaans paard) verschilt van een virus doordat de gebruiker van de computer een handeling moet verrichten (zoals het downloaden van een aangeboden bestand) om het programma te installeren. In dit geval werd de opdracht tot installatie door de verdachten gegeven.
6 Het onder 3 tenlastegelegde lijkt centraal te stellen dat de geïnfecteerde computers vervolgens herstarten en/of crashen. Als ik het goed begrijp vindt het crashen en herstarten echter plaats op het moment waarop het Toxbot-virus de computer infecteert. Het gaat om de methode waarmee de beveiliging wordt doorbroken of omzeild en is dus inherent aan het onder 1 tenlastegelegde hacken. Zie bewijsmiddel 9 (p. 22) en bewijsmiddel 17 (p. 30).
7 Stb 2006, 300; iwtr. Stb 2006, 301.
8 NLR, aant. 1 op art. 157; Smidt II (2e druk), p. 118.
9 Vgl. NLR, aant. 9 op art. 157.
10 Met betrekking tot art. 157 Sr wordt aangenomen dat er gemeen gevaar is zodra meer dan één goed, onverschillig welk, aan de gevolgen van de gevaar veroorzakende gebeurtenis blootstaat. Zie NLR, aant. 9 op art. 157.
11 Wellicht leverde de vernieling waarmee werd gedreigd, wel gemeen gevaar voor de verlening van diensten op. Maar daarin voorzag art. 285 Sr, waarop de vervolging was gebaseerd, destijds niet. Dit veranderde door toevoeging van het bestanddeel "gemeen gevaar voor verlening van diensten" aan art. 285 Sr bij de Wet computercriminaliteit II (Stb. 2006, 300). Vgl. TK 1998-1999, 26 671, nr. 3 (MvT), p. 47 waarin verwezen wordt naar het genoemde arrest.
12 Dit tweede lid is toegevoegd bij de Tweede nota van wijziging. Zie TK 1991-1992, 21551, nr. 11, pp. 10 en 24 en nr. 12, p. 2 en 6/7.
13 Het onder punt 3 omschreven gedrag is niet als het meermalen medeplegen van het misdrijf van art. 350a Sr aan de verdachte tenlastegelegd. Dat geldt ook voor het in art. 350a lid 3 Sr omschreven misdrijf.
14 Zie TK 1990-1991, 21551, nr. 7, p. 5. De strafbaarstelling werd toegevoegd bij de Nota van wijziging en was aanvankelijk vervat in het tweede lid van art. 350a Sr. De Tweede nota van wijziging scherpte de tekst aan en vernummerde de bepaling. Zie TK 1991-1992, 21551, nr. 12, p. 7.
15 Ik spreek van een bijkomend argument omdat de tenlastegelegde feiten anterieur zijn aan de onderhavige wetswijziging. Hetgeen in de MvT wordt gesteld, kan gezien worden als een bevestiging van hetgeen daarvoor reeds geldend recht was.
16 Rapport van de Commissie computercriminaliteit, Informatietechniek & strafrecht, Staatsuitgeverij/ministerie van Justitie 1987, p. 59.
17 A.w., pp. 59 en 60.

18 Erg sterk lijkt mij dit argument niet te zijn. Als men zich per ongeluk de toegang verschaft, is van het in de term "binnendringen" besloten liggende opzet geen sprake. Een extra drempel is dus niet nodig om het per ongeluk kennisnemen van opgeslagen gegevens straffeloos te doen zijn.
19 A.w., p. 59.
20 TK 1989-1990, 21 551, nr. 3 (MvT), p. 16, 17.
21 TK 1990-1991, 21551 nr. 7, p. 1.
22 TK 1990-1991, 21551 nr. 6, p. 28. Zie ook p. 10 en p. 12.
23 Idem, pp. 28 en 29.
24 Idem, p. 32.
25 Idem, pp. 9 en 10.
26 Idem, pp. 28, 29.
27 Dit wordt nog toegelicht met behulp van het volgende voorbeeld. Een zeer geheim staatsdocument in een dichtgeplakte envelop is naar geldend recht beschermd omdat het openscheuren van die envelop zaaksbeschadiging oplevert. Het lezen van een in de trein achtergelaten geheim staatsdocument dat niet in een envelop zit, is niet strafbaar, ook als staat daar levensgroot 'geheim' op. Voorgesteld wordt, aldus de Minister, om de kennisneming van digitale gegevens op dezelfde voet strafbaar te stellen. Alleen de mededeling van de beheerder van het geautomatiseerde werk dat de gegevens niet toegankelijk ("geheim") zijn, is voor strafbaarheid onvoldoende. Maar zo gauw er iets meer is (de envelop), is kennisneming wel strafbaar, hoe inadequaat de beveiliging ook is.
28 TK 1990-1991, 21551, nr. 7, p. 4.
29 EK 1992-1993, 21551, nr 39a, p. 5.
30 Eenduidig is de wetsgeschiedenis overigens niet. In de Nota naar aanleiding van het Eindverslag (TK 1991-1992, 21551, nr 11, p. 17) wordt gesteld dat de strafbaarstelling mede omvat "het binnendringen in een systeem waarbij formeel geen beveiliging wordt doorbroken maar waarvoor wel valse signalen, een valse sleutel of een valse hoedanigheid wordt aangewend".
31 A.w., p. 60. In de MvT worden de begrippen niet toegelicht.
32 Vgl. A.E. Harteveld en G. Knigge, Taal en teken, DD 1991, p. 121.
33 Afgaande op onder meer Wikipedia is identificatie de eerste stap in elk autorisatieproces. De tweede stap is authenticatie. De derde stap autorisatie.
34 Het artikel werd ingevoegd bij de Nota van wijziging. De Tweede nota van wijziging voorzag in een verbeterde redactie.
35 TK 1987-1988, 20369, nr.3, p. 53 e.v. Verwezen wordt kennelijk naar de p. 69 van het Rapport van de Commissie Franken, alwaar wordt voorgesteld aan art. 326 Sr toe te voegen de zinsnede 'of het verrichten van enige dienst'. Op de specifieke vorm van computerfraude die in art. 50 lid 3 Wet op de telecommunicatievoorzieningen werd strafbaar gesteld, wordt in het rapport niet ingegaan.
36 TK 1990-1991, 21551, nr. 7, pp. 4, 5.
37 TK 1991-1992, 21551, nr 12, p. 3 e.v.
38 TK 2004-2005, 26671, nr. 7, p. 32 e.v.
39 Zie de Tweede nota van wijziging, TK 2004-2005, 26671, nr. 7, p. 31 e.v. en de MvA aan de Eerste Kamer, EK 2005-2006, 26671, D, p. 1 e.v.
40 In dezelfde zin B.J. Koops, Strafrecht en ICT, 2e druk, Sdu uitgevers, Den Haag 2007, p. 32. Ik laat nog daar dat het Kaderbesluit autonome begrippen kent, zodat een eventueel scherp onderscheid dat naar nationaal recht tussen het doorbreken van een beveiliging en (bijvoorbeeld het onbevoegd gebruik van toegangscodes) zou moeten worden gemaakt, voor de toetsing aan dat Kaderbesluit van weinig betekenis is.

Open het oorspronkelijke document