

## Stroomschema's computercriminaliteit

In het Wetboek van Strafrecht staan een aantal delicten waarbij geautomatiseerde werken<sup>1</sup> en gegevens<sup>2</sup> centraal staan. Die delicten zijn met de Wet Computercriminaliteit en de Wet Computercriminaliteit II in het strafrecht geïntroduceerd.

De aanpak van cybercrime wordt soms gezien als moeilijk, ingewikkeld en iets van enkel specialisten. Niets is minder waar; waar delen van ons leven digitaal zijn, zijn delen van criminaliteit dat ook. Computervredebreuk is in de basis niet anders dan huisvredebreuk: de dader is ergens geweest waar hij niet mag zijn. En een DDoS-aanval op een school zodat de website onbereikbaar wordt, is in de basis niet anders dan het versperren van de deuren van die school zodat de leerlingen niet naar binnen kunnen.

Het kan soms lastig zijn om – naar aanleiding van een aangifte of dossier – te bepalen welke strafbaarstelling aan de orde is. De stroomschema's in deze factsheet zijn bedoeld om te helpen bij die beoordeling.

Twee andere nuttige hulpbronnen bij de beoordeling van computercriminaliteit zijn door de politie ontwikkeld.

Op de kennisomgeving van de politie (Kompol) staat de 'Cybertoolkit'. Die toolkit is gebaseerd op het boek 'Alledaags politiewerk in een gedigitaliseerde wereld - Handreiking voor delicten met een digitale component' uit 2015. De Cybertoolkit op Kompol wordt actueel gehouden.

[http://kompol.politieacademie.politie.nl/topic.aspx?id=Topics/1\\_cybertoolkit\\_home.toolbox.dita](http://kompol.politieacademie.politie.nl/topic.aspx?id=Topics/1_cybertoolkit_home.toolbox.dita)

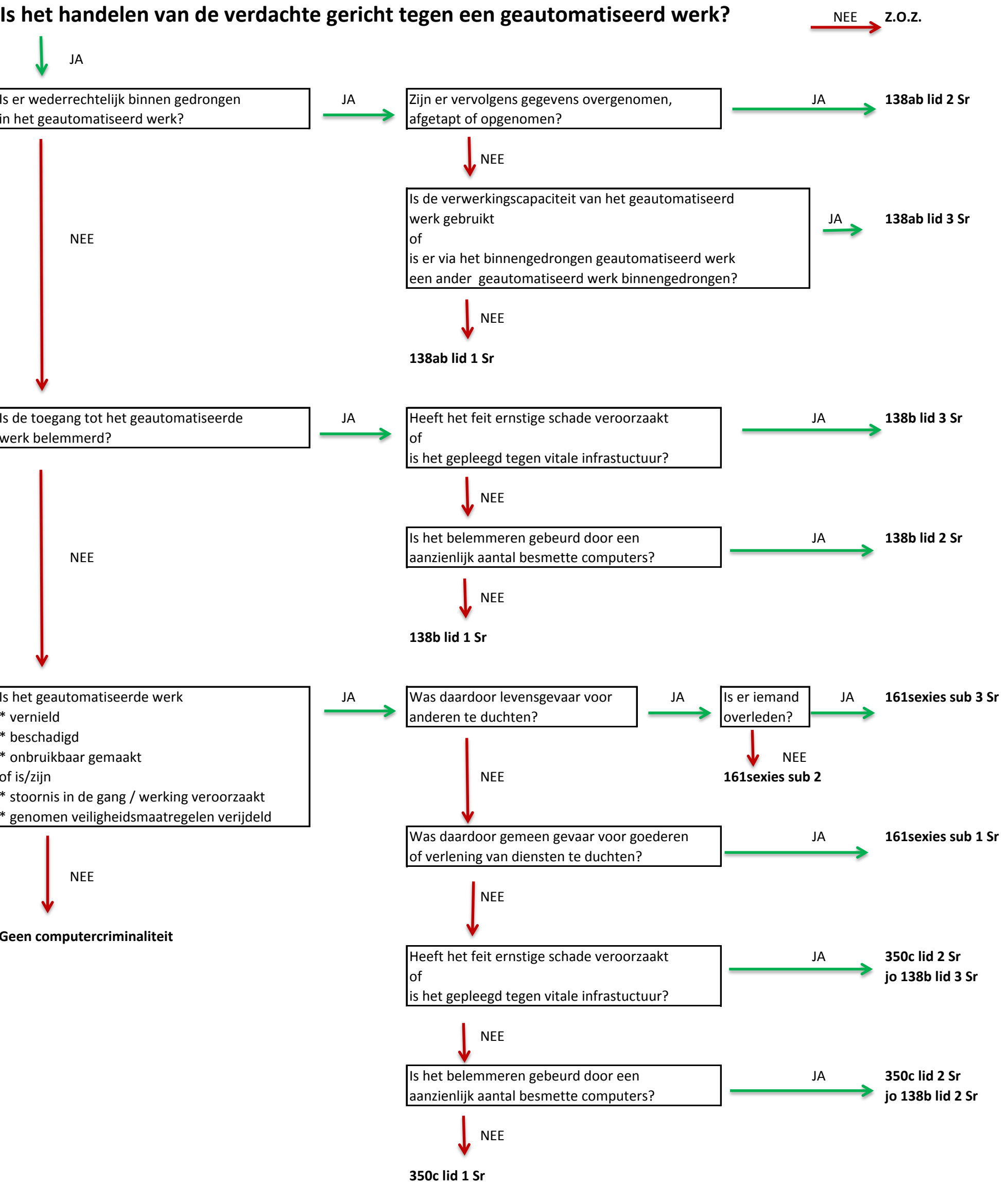
Verder staat op <https://webapps.politieacademie.nl/naslagwerk/cybercrime> een webapp met informatie over het herkennen en opsporen van cybercrime.

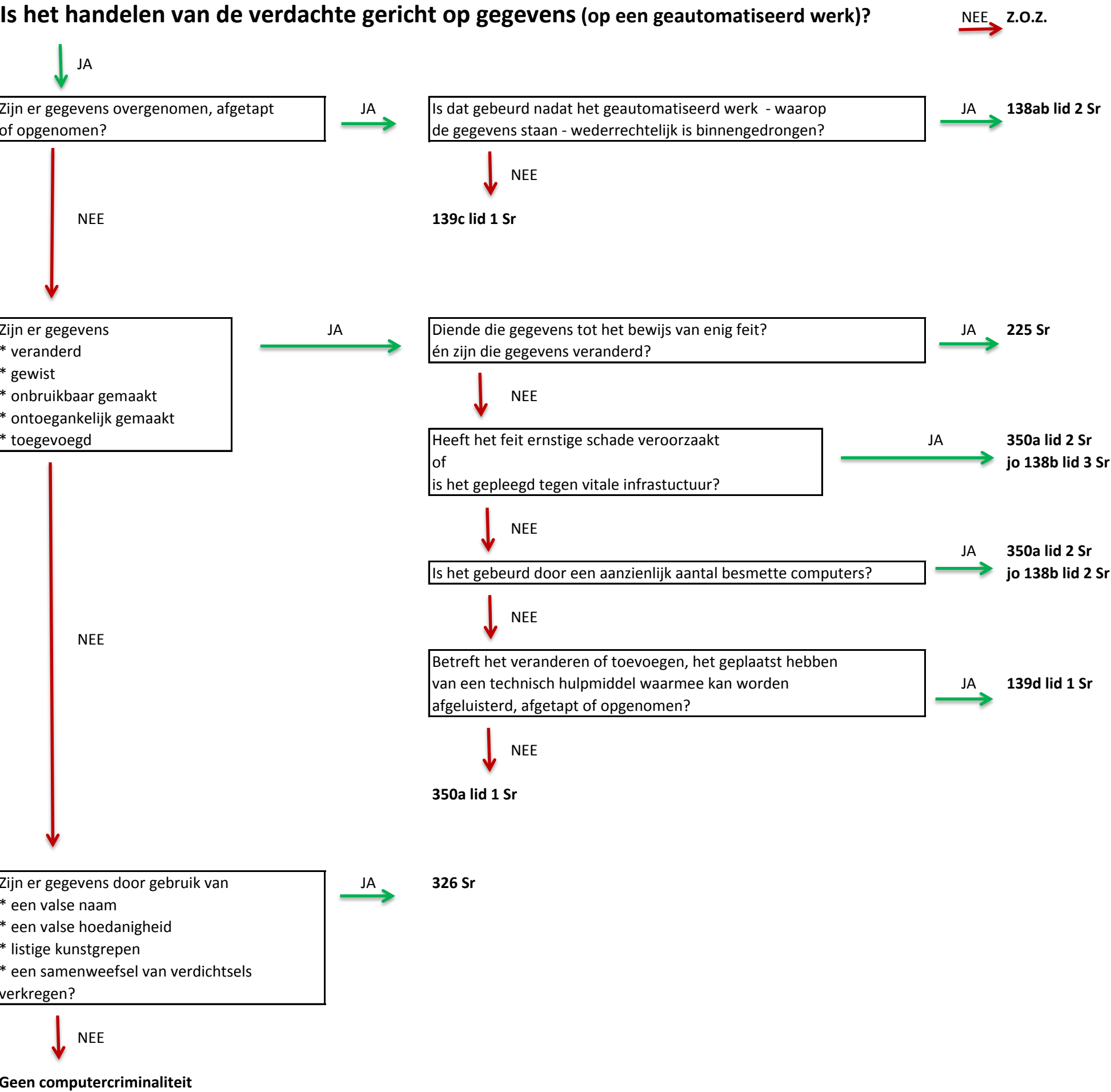
11 september 2017  
Jesse van der Putte

---

<sup>1</sup> In artikel 80sexies Sr staat de definitie van een geautomatiseerd werk. Daaronder vallen bijvoorbeeld computers, smartphones, servers en tablets. Maar ook een internetbankieren omgeving, een mail-account en een OV-chipkaart.

<sup>2</sup> In artikel 80quinquies Sr staat de definitie van gegevens. Die definitie is heel breed. De inhoud van een geautomatiseerd (de bestanden op een computer of mails op een telefoon) valt er in het algemeen onder.

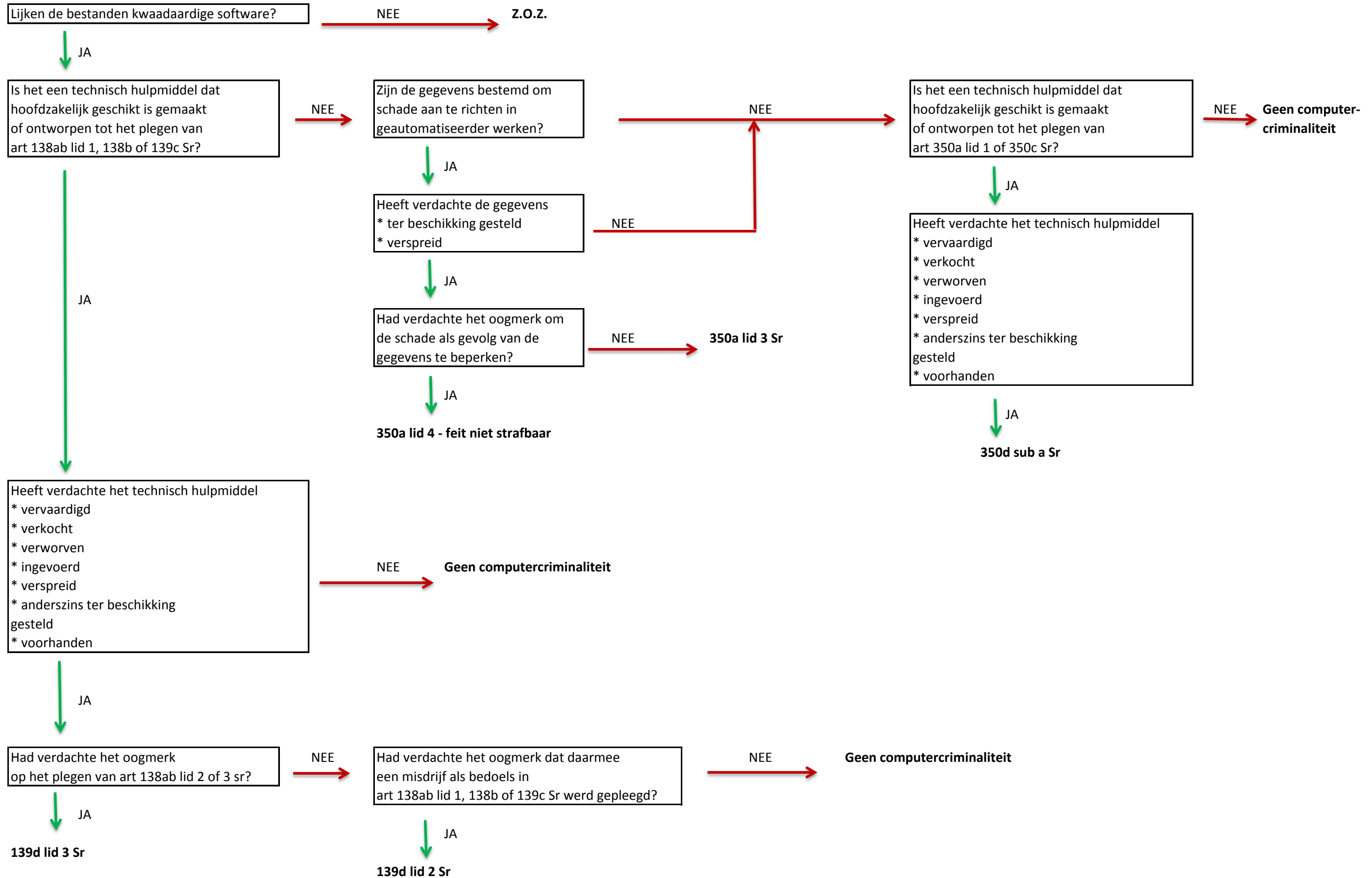




# Cybercrime

## malware

Er zijn verdachte bestanden aangetroffen op een gegevensdrager van de verdachte



Cybercrime

gekopieerde gegevens

Er zijn verdachte bestanden aangetroffen op een gegevensdrager van de verdachte

Lijken de bestanden kwaadaardige software?

JA → Z.O.Z.

NEE ↓

Zijn de bestanden  
\* een wachtwoord  
\* een toegangscode  
\* of daarmee vergelijkbaar?

JA ↓

Kan met die gegevens toegang  
worden verkregen tot een  
geautomatiseerd werk?

JA ↓

Heeft verdachte de gegevens  
\* vervaardigd  
\* verkocht  
\* verworven  
\* ingevoerd  
\* verspreid  
\* anderszins ter beschikking gesteld  
\* voorhanden

JA ↓

Heeft verdachte het oogmerk om met die  
gegevens art 138ab, 138b of 139c Sr te  
overtreden?

JA ↓

139d lid 2 Sr

NEE →

Zijn de gegevens verkregen door  
wederrechtelijk af luisteren,  
aftappen of opnemen?

JA ↓

Heeft verdachte de gegevens bekend gemaakt?

JA ↓

139e sub 2 Sr

NEE →

Geen computercriminaliteit

NEE →

Staan de gegevens  
op een voorwerp?

NEE →

Geen computercriminaliteit

JA ↓

Heeft verdachte het voorwerp aan  
een ander ter beschikking gesteld?

JA →

139e sub 3 Sr

NEE ↓

Kon verdachte over het  
voorwerp beschikken?

JA →

139e sub 1 Sr

NEE ↓

Geen computercriminaliteit

NEE →

Geen computercriminaliteit

NEE →

Heeft verdachte het oogmerk om met die  
gegevens art 350a lid 1 of 350c Sr te  
overtreden?

JA ↓

350d sub a Sr

NEE →

Geen computercriminaliteit