Bijlage III: Begrippenlijst

Bij het toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

CTIVD nr. 70

[vastgesteld op 19 augustus 2020]

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 70

BIJLAGE III

Bij het toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

Begrippenlijst

Deze lijst licht een aantal begrippen toe dat wordt gebruikt in het toezichtsrapport. De CTIVD heeft bij de gegeven omschrijvingen geen volledigheid nagestreefd, maar geprobeerd de lezer een zo concreet mogelijk beeld te geven van de betreffende begrippen.

Aantekening houden	De wettelijke verplichting dat van de uitoefening van een bevoegdheid aantekening wordt gehouden, ook wel aangeduid als verslaglegging (artikel 31 Wiv 2017). Hieraan kan op verschillende manieren invulling worden gegeven.
Behoorlijkheid	Algemeen vereiste van gegevensverwerking (artikel 18 lid 2 Wiv 2017). Hieronder valt onder meer een weging tussen het doel van de verstrekking en de nadelen ervan voor personen of organisaties wiens gegevens worden verstrekt.
Bulkdataset	Een grote gegevensverzameling waarvan het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden.
Bulkhack	Het verzamelen van een bulkdataset met de hackbevoegdheid.
CNE	Computer Network Exploitation. In het kader van het huidige onderzoek duidt deze term een afdeling van de Joint Sigint Cyber Unit (JSCU) aan, die gespecialiseerd is in het binnendringen in geautomatiseerde werken.
Doelwit	In het kader van het huidige onderzoek wordt het begrip doelwit gebruik om de persoon of organisatie aan te duiden waarop de inzet van de hackbevoegdheid is gericht. Doelwitten kunnen dus zowel targets als non-targets zijn.
Functie- (en/of taak) scheiding	Het beperken van toegang tot gegevens op basis van de functie en/of de taak van dienstmedewerkers. Het betreft het bij uitzondering van anderen kennis kunnen nemen van bepaalde gegevens op basis van de taken die aan de functie van deze medewerker zijn toebedeeld.

Fundamentele rechten	Grondrechten die o.a. zijn neergelegd in internationale verdragen en uitgelegd in jurisprudentie, zoals het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Voorbeelden van deze rechten zijn het recht op eerbiediging van privé-, familie- en gezinsleven (privacy), vrijheid van meningsuiting en het recht op vrijheid en veiligheid.
Geautomatiseerd werk	Een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken. Voorbeelden zijn computersystemen, -netwerken en smartphones.
Hackbevoegdheid	De bevoegdheid tot het mogen verkennen van en binnendringen in een geautomatiseerd werk (artikel 45 Wiv 2017).
Inlichtingendienst	Een dienst die onderzoek doet naar andere landen om (potentiële) dreigingen voor de eigen nationale veiligheid te onderkennen.
JSCU	Joint Sigint Cyber Unit. Een gezamenlijke eenheid van de AIVD en de MIVD die zich bezighoudt met de verwerking van gegevens op het gebied van *signals intelligence* (sigint) en cyber.
Logboek	Een logboek waarin dienstmedewerkers handmatig onder meer handelingen, afwegingen en gebeurtenissen vastleggen.
Logging	Stelselmatig geautomatiseerde registratie van gegevens van het gebruik en de werking van een computerprogramma.
Non-target	Non-targets zijn niet zelf in onderzoek bij de diensten, maar staan in een bepaalde (bijvoorbeeld persoonlijke of zakelijke) relatie tot een target.
Noodzakelijkheid	Algemeen vereiste van gegevensverwerking. De verwerking moet een bepaald doel dienen en kunnen bijdragen aan de verwezenlijking van dit doel (artikel 18 lid 1 Wiv 2017).
Onrechtmatig	Een beoordeling van het handelen van de AIVD en/of de MIVD. Bij het oordeel onrechtmatig is er sprake van strijdigheid met wet- en regelgeving. Deze wet- en regelgeving bestaat uit de Wiv 2017, jurisprudentie en door de ministers naar aanleiding van eerdere toezichtsrapporten overgenomen aanbevelingen. Bij de beoordeling wordt rekening gehouden met de aard van de belangen waarop een inbreuk wordt gemaakt en met de mate van de inbreuk.
OOG-interceptie	Onderzoeksopdrachtgerichte interceptie. Deze bijzondere bevoegdheid tot interceptie van elke vorm van telecommunicatie of gegevensoverdracht is in de Wiv 2017 in een stelsel van drie fasen opgenomen: (1) de interceptie door de Joint Sigint Cyber Unit (artikel 48 Wiv 2017), (2) de optimalisatie van het interceptie- en selectieproces (artikel 49 Wiv 2017) en (3) de analyse van de inhoud van de communicatie en metadata (artikel 50 Wiv 2017).

Operator	In het kader van het huidige onderzoek duidt deze term een gespecialiseerde medewerker van de afdeling Computer Network Exploitation aan, die belast is met de uitvoering van de hackbevoegdheid.
Opruimplicht	De wettelijke inspanningsverplichting tot het verwijderen van technische hulpmiddelen die bij de uitoefening van de hackbevoegdheid (specifiek het binnendringen in een geautomatiseerd werk) zijn gebruikt (artikel 45 lid 7 Wiv 2017).
Persoonsgegevens	Gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individuele natuurlijke persoon (bijvoorbeeld een naam of een foto). Artikel 1, aanhef en onder e, Wiv 2017.
Protocolplicht	De verplichting voor de AIVD en de MIVD om inzichtelijk bij te houden welke gegevens(bestanden) in het kader van de samenwerkingsverbanden worden uitgewisseld.
Relevantie	Gegevens zijn relevant als de gegevens betekenis hebben voor het onderzoek waarvoor ze zijn verworven, dan wel voor enig ander lopend onderzoek. Bij het beoordelen van de relevantie van gegevens moet inhoudelijk worden gekeken 'of de gegevens in positieve zin bijdragen aan het onderzoek, alsook of die gegevens bepaalde vragen negatief kunnen beantwoorden, hypothesen kunnen ontkrachten of anderszins van doorslaggevend belang zijn' (artikel 27 Wiv 2017).
Target	Een persoon of organisatie waar de AIVD of MIVD onderzoek naar verricht.
Technisch kenmerk	Kenmerk dat herleidbaar is tot verschillende elementen van (tele) communicatie, bijvoorbeeld een telefoonnummer of een e-mailadres. Technische kenmerken kunnen als selectiecriterium worden gebruikt.
Tekortkoming	Een punt van verbetering voor de toekomst. Het vastgestelde gebrek is niet van zodanig gewicht of ernst dat het (al) leidt tot het oordeel onrechtmatig.
Toestemmingsverzoek	Het document waarin de verstrekking wordt gemotiveerd en wat wordt voorgelegd aan de betreffende minister voor de toestemming voor de gegevensverstrekking.
TIB	Toetsingscommissie Inzet Bevoegdheden, een commissie die vooraf toetst of de inzet van specifieke bijzondere bevoegdheden door de AIVD en de MIVD rechtmatig is. Het oordeel van de TIB is bindend.
Veiligheidsdienst	Een dienst die onderzoek doet naar personen en organisaties die mogelijk een gevaar vormen voor het voortbestaan van de democratische rechtsorde, voor de veiligheid of voor andere gewichtige belangen van de staat, dan wel voor de veiligheid en de paraatheid van de krijgsmacht.
Verslaglegging	Zie onder 'Aantekening houden'.
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002. Deze wet is met de inwerkingtreding van de Wiv 2017 op 1 mei 2018 opgehouden.

Wiv 2017	Wet op de inlichtingen- en veiligheidsdiensten 2017. Deze wet is op 1 mei 2018 in werking getreden.
Zorgvuldigheid	Algemeen vereiste van gegevensverwerking. Het borgen van de inhoudelijke juistheid en de correcte weergave van de gegevens die worden verstrekt (artikel 18 lid 2 Wiv 2017).

Oranjestraat 15, 2514 JB Den Haag
Postbus 85556, 2508 CG Den Haag

T 070 315 58 20
E info@ctivd.nl | www.ctivd.nl