Prof. dr. B.P.F. Jacobs & mr. drs. R.H.T. Jansen[1]

Hoe hackers vastlopen

Over uitvoeringsproblemen bij hackoperaties van de politie en van de inlichtingen- en veiligheidsdiensten

Computerrecht 2024/3

Verschillende rapporten tonen aan dat er uitvoeringsproblemen zijn ontstaan bij hackoperaties van de politie en van de inlichtingen- en veiligheidsdiensten. In deze bijdrage wordt gereflecteerd op die rapporten en op de achterliggende problematiek, die samen lijkt te hangen met de mate van gedetailleerdheid en de interpretatie van de toepassingsvoorwaarden. De parallellen tussen beide domeinen komen hier aan bod, maar de nadruk ligt op hackoperaties van de AIVD en de MIVD. Op dit moment vormen die operaties namelijk onderwerp van politieke discussie.

1. Inleiding

Hacken is een belangrijke bevoegdheid, zowel voor de politie als voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Zo kunnen deze autoriteiten controle verkrijgen over (een deel van) een computer, smartphone of ander apparaat en vervolgens informatie op dat apparaat inzien, bepaalde communicatie afluisteren of gegevens ontoegankelijk maken. Hacken heeft grote operationele waarde, zeker in een tijdperk waarin communicatie steeds beter is versleuteld.[2] De inzet van dit instrument ligt echter gevoelig. Het is immers risicovol, verstrekkend en tegenwoordig misschien wel 'de zwaarst denkbare inbreuk op de privacy'.[3] Om een indruk te geven van de potentie en de relevantie ervan: Ridouan Taghi is vermoedelijk via een hackoperatie gelokaliseerd in Dubai.[4]

De afgelopen tijd zijn verschillende onderzoeken uitgevoerd naar hackoperaties. Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC),[5] de procureur-generaal bij de Hoge Raad (PG-HR)[6] en de Inspectie Justitie en Veiligheid (Inspectie)[7] rapporteerden over de opsporingscontext. De Evaluatiecommissie WIV 2017 (Commissie-Jones-Bos)[8] de Algemene Rekenkamer[9] en – al iets eerder – de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)[10] analyseerden de inzet in de nationale veiligheidscontext. De rapporten zijn stuk voor stuk de moeite van het lezen waard. De gemene deler is dat er 'problemen' in de toepassingspraktijk en 'patstellingen' met toezichthouders zijn ontstaan.

Wij grijpen die rapporten aan om te reflecteren op de uitvoering van de hackbevoegdheid. Wat zijn de voornaamste problemen? Waardoor ontstaan die? En hoe zouden die kunnen worden opgelost? Wij beschrijven hier beide werkvelden en zoeken naar parallellen daartussen, maar richten ons vooral op de AIVD en de MIVD. Want terwijl de cyberdreiging toeneemt, staat hun cyberslagkracht onder druk. Zozeer zelfs, dat de regering de normering van bepaalde hackoperaties tijdelijk wil oprekken en het toezicht wil verschuiven van de voorkant (*ex ante*) naar de

1 Prof. dr. B.P.F. (Bart) Jacobs is hoogleraar Beveiliging, privacy en identiteit aan de Radboud Universiteit, lid van de CTIVD-kenniskring, lid van de Wetenschappelijke Adviesraad Politie en voormalig lid van de Evaluatiecommissie Wiv 2017. Mr. drs. R.H.T. (Rowin) Jansen is promovendus Algemene rechtswetenschap aan de Radboud Universiteit en schrijft een proefschrift over het toezicht op de AIVD en de MIVD. De kopij is afgerond op 6 december 2023.

2 Zie ook Adviesbrief inzake reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie, anders dan inperking van encryptie van de Cyber Security Raad, d.d. 23 augustus 2022.

3 B.J. Koops e.a., *Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX*, Tilburg 2016, p. 103.

4 Vgl. 'AIVD gebruikt omstreden Israëlische hacksoftware', *de Volkskrant* (2 juni 2022); 'AIVD gebruikt omstreden Israëlische hacksoftware, ook voor hacken Ridouan Taghi', *NOS* (2 juni 2022).

5 A. van Uden & C.A.J. van den Eeden, *De hackbevoegdheid in de praktijk. Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126 zpa Sv)*, Den Haag: WODC 2022 (hierna WODC 2022). Zie ook J.J. van Berkel, A. van Uden & J.H. Goes, *De hackbevoegdheid in het buitenland. Een rechtsvergelijkend onderzoek naar wettelijke regelingen en waarborgen omtrent de kwaliteit van gegevens*, Den Haag: WODC 2023 (hierna WODC 2023). Onlangs is deze naam gewijzigd in Wetenschappelijk Onderzoek- en Datacentrum.

6 Procureur-generaal bij de Hoge Raad der Nederland, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie*, Den Haag 2022 (hierna PG HR 2022).

7 Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2022*, Den Haag 2023 (hierna Inspectie 2023).

8 Evaluatiecommissie WIV 2017, *Wet op de inlichtingen- en veiligheidsdiensten 2017. Evaluatie 2020*, Den Haag 2021 (hierna ECW 2021).

9 Algemene Rekenkamer, *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt*, Den Haag 2021 (hierna ARK 2021).

10 CTIVD, *Toezichtsrapport nr. 53 over de inzet van de hackbevoegdheid*, Den Haag 2017 (hierna CTIVD 2017); CTIVD, *Toezichtsrapport nr. 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*, Den Haag 2020 (hierna CTIVD 2020).

achterkant (*ex durante* en *ex post*).[11] Zij regelt dat in de bij het parlement aanhangige 'Cyberwet' en loopt daarmee vooruit op een herziening van de Wet op de inlichtingen en veiligheidsdiensten 2017 (Wiv 2017).[12]

De opzet is als volgt. Na een introductie van het fenomeen 'hacken' (§ 2), schetsen wij het geldend recht (§ 3). Vervolgens staan vier thema's centraal: autorisatie (§ 4), kwetsbaarheden en technische risico's (§ 5), technische hulpmiddelen (§ 6) en toezicht (§ 7). Wij sluiten af met een slotbespiegeling (§ 8). Alvast de rode draad: onze taxatie is dat de wetgever schone handen probeert te houden op een gebied dat per definitie rommelig is. De wetgever lijkt hackoperaties juridisch dicht te willen spijkeren. In de opsporingscontext resulteert dat in minutieuze toepassingsvoorwaarden.[13] Hacken is echter een dynamisch proces, met een hoge mate van onvoorspelbaarheid. Reguleringsdrang leidt dan al snel tot uitvoeringsproblemen. In het nationale veiligheidsdomein zitten de problemen veeleer in de interpretatie van regels en is een verschuiving in het toezicht wenselijk.

Een laatste opmerking vooraf. Ons doel is om met deze bijdrage enig tegenwicht te bieden aan het huidige controledenken en de verdere juridisering van hacken. Wij leggen hier daarom de nadruk op de uitvoerbaarheid van deze cyberbevoegdheid. Omdat het in dit bestek niet mogelijk is alle juridische en technische finesses volledig uit te diepen, chargeren wij zo nu en dan, welbewust.

2. Hacken: nut en noodzaak

Politie- en inlichtingenwerk is informatiegestuurd. Veel informatie komt uit open bronnen. Voor menig onderzoek is echter ook toegang tot afgeschermde informatie nodig. Vaak kan die toegang worden verkregen door de versleuteling van die informatie te doorbreken. Moderne versleuteling is in principe onkraakbaar. Gegevens zijn in elk geval versleuteld tijdens transport en soms ook tijdens opslag. Tijdens gebruik (lezen, schrijven, aanpassen) zullen gegevens echter beschikbaar moeten zijn voor de gebruiker. Die gebruiksfase biedt een *window of opportunity* om, zonder toestemming van de rechthebbende, bij bepaalde gegevens te komen.

Daar zijn verschillende methoden voor. Een hacker dringt meestal binnen via een slecht beveiligde 'poort' op het apparaat zelf. Dat beveiligingsgebrek is vaak een fout in de hard- of software, die via die poort bereikbaar is. Hacken kan ook indirect verlopen, via één of meer buur-computers, of via het hacken van een leverancier van (beveiligings)-software die op het doelapparaat wordt gebruikt. Voort is het (technisch) mogelijk de hele digitale inbraak uit te besteden aan een externe partij.

Net als een inbreker, wil een hacker niet worden ontdekt. Zoiets kan immers leiden tot repercussies en terughackacties. Er is dan ook een intrinsieke motivatie om risico's te minimaliseren. Een belangrijk verschil is dat de hacker geen last heeft van fysieke zicht- of hoorbaarheid. Bij digitaal binnendringen is de tijdsdruk doorgaans ook wat minder. De complexiteit en de onvoorspelbaarheid van de activiteiten zijn daarentegen groter, omdat vaak meerdere lagen van beveiliging, op verschillende apparaten, moeten worden doorbroken. Waar een inbreker zich redelijk goed kan voorbereiden door middel van voorafgaande observatie, kan een hacker dat in veel mindere mate – de voorbereidingen zijn sterker geïntegreerd met het binnendringen zelf. Hacken vergt dan ook kennis, ervaring, geduld, improvisatie en *out-of-the-box*-denken.

De politie en de diensten hacken om verschillende redenen. Opsporingsambtenaren kunnen dit instrument inzetten tegen individuele verdachten, maar ook tegen versleutelingsmechanismen die criminele groeperingen gebruiken. Zo vindt hacken plaats in de strijd tegen de georganiseerde criminaliteit, terrorisme, seksueel kindermisbruik of computervredebreuk.[14] Omdat de aangetroffen informatie later mogelijk zal worden gebruikt in een strafzaak, is het belangrijk dat die informatie betrouwbaar, herleidbaar en integer is.[15] Tot op heden hackt de politie met name mobiele telefoons.[16] Dat leverde vooral sturingsinformatie op, die, in tegenstelling tot sommige verwachtingen, dus niet hét bewijs in een opsporingsonderzoek of tijdens een berechting vormde.[17]

Waar politie en justitie aan bewijsgaring en bewijsvoering doen, mogen de diensten hacken indien dat in het belang van de nationale veiligheid noodzakelijk is.[18] Met dit instrument kunnen zij bijvoorbeeld gericht informatie van en over bepaalde targets verzamelen, een aanvalsinfrastructuur inzichtelijk maken of een strategische informatiepositie opbouwen.[19] In veel gevallen is het te doen om targets die zich in een ander land bevinden of die handelen ten dienste van een buitenlands regime. De Cyberwet

11 Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma (Kamerdossier 36263). De regering geeft daarmee ook uitvoering aan de motie-Van der Staaij c.s. (*Kamerstukken II* 2021/22, 36045, nr. 16). Wij schreven een reactie op het wetsvoorstel in internetconsultatie en een position paper voor het rondetafelgesprek met de vaste commissie voor Binnenlandse Zaken op 5 april 2023. Onze inbreng is raadpleegbaar via de website van de Tweede Kamer. Zie ook R.H.T. Jansen, 'Van accentverschuiving naar stelselwijziging. Toezicht in het conceptvoorstel Tijdelijke cyberwet voor de AIVD en de MIVD', *NJB* 2022/2096, afl. 30, p. 2406-2416; S.A.M. Harleman, 'Een tijdelijke Cyberwet maakt nog geen sleepwet', *NJB* 2022/2695, afl. 38, p. 3120-3127.

12 *Kamerstukken II* 2022/23, 36263, nr. 3, p. 10-12. De wetgever wil voor wat betreft het toezichtstelsel echter geen fait accompli scheppen. Wij zien de Cyberwet dan ook als een 'experimenteerwet'. Vgl. *Kamerstukken II* 2022/23, 34588, nr. 92, par. 5.4.

13 Zie ook Y. Buruma, 'Wettelijke hackbevoegdheden', *NJB* 2022/2545, afl. 36, p. 2965.

14 *Kamerstukken II* 2023/24, 34372, nr. 31, p. 1-2.

15 Vgl. WODC 2022, p. 139.

16 WODC 2022, p. 89.

17 Geen enkele inzet is inhoudelijk behandeld door een zittingsrechter. Zie WODC 2022, p. 14, 143-145 en 166-167.

18 Artikel 8 (AIVD) en artikel 10 (MIVD) Wiv 2017.

19 *Kamerstukken II* 2022/23, 36263, nr. 3, p. 6.

ziet niet zonder reden op hackoperaties tegen landen met een op Nederland gericht offensief cyberprogramma, waaronder China, Rusland, Iran en Noord-Korea.[20]

3. Hacken als wettelijke bevoegdheid

3.1 *Algemeen*

Hacken heet juridisch het 'binnendringen van een geautomatiseerd werk'. Daarbij mogen een technische ingreep, valse signalen, valse sleutels, een valse hoedanigheid of een applicatie worden gebruikt.[21] Het inloggen op een geautomatiseerd werk met inloggegevens die zijn ontfutseld aan de gebruiker, bijvoorbeeld via *social engineering*, kwalificeert eveneens als binnendringen.[22] Een geautomatiseerd werk is 'een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken'.[23] Die definitie omvat in elk geval computers, servers, modems, routers, smartphones en tablets, maar ook andere apparaten die in verbinding staan met een netwerk zoals navigatiesystemen, televisies of auto's.[24]

Het Wiv-regime kent een harde, maar enigszins gekunstelde knip tussen 'verkennen' en 'binnendringen'. Verkennen duidt op het in kaart brengen van eigenschappen zoals open netwerkpoorten, geïnstalleerde software, aanwezige netwerkverbindingen en onderliggende hardware.[25] Zo kunnen de diensten een *up to date* beeld krijgen van de buitenste schil van de digitale omgeving van het onderzoeksobject, eventuele zwakheden in systemen ontdekken en verder richting geven aan de geplande operatie. Pas daarna kan het daadwerkelijke binnendringen starten. Verkennen heeft, kortom, een voorbereidend en ondersteunend karakter.[26] In het Wetboek van Strafvordering is verkennen niet aangemerkt als afzonderlijke bevoegdheid, maar uiteraard verrichten ook opsporingsambtenaren verkennende activiteiten ten behoeve van het latere binnendringen.[27]

3.2 *Opsporingsdomein*

Sinds de inwerkingtreding van de Wet computercriminaliteit III mag de officier van justitie opsporingsambtenaren bevelen om te hacken bij een verdenking van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, bij ernstige misdrijven in georganiseerd verband of bij aanwijzingen van een terroristisch misdrijf.[28] Zo is een leemte in het instrumentarium opgevuld. Het idee is ook dat opsporingsambtenaren via deze route het versleutelprobleem in opsporingsonderzoeken kunnen omzeilen en eventuele problemen rondom *cloud computing* kunnen tegengaan.[29]

Hacken is wel een 'paraplubevoegdheid' genoemd.[30] Na het binnendringen mag de politie namelijk verschillende onderzoekshandelingen verrichten. Dat zijn (a) het vaststellen en vastleggen van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals identiteit of locatie, (b) het opnemen of aftappen van (vertrouwelijke) communicatie, (c) het stelselmatig observeren, (d) het vastleggen van opgeslagen gegevens en (e) het ontoegankelijk maken van bepaalde gegevens.[31] De toepassingsregels zijn neergelegd in het Wetboek van Strafvordering (Sv), de Wet politiegegevens (Wpg) en het – uiterst gedetailleerde – Besluit onderzoek in een geautomatiseerd werk (Bogw).[32]

Het hacken is belegd bij één technisch team: het Digital Intrusion Team van de Landelijke Eenheid van de Nationale Politie.[33] Deze 'Digit-politie' wordt aangestuurd door het 'Digit-OM'. Dat is ondergebracht bij het Landelijk Parket van het Openbaar Ministerie. Naast deze technische actoren spelen ook tactische actoren een rol. De hackoperatie vindt namelijk altijd plaats binnen een al lopend onderzoek. Dat onderzoek wordt uitgevoerd door een tactisch team, bijvoorbeeld een team van de districtsrecherche of Team High Tech Crime, onder gezag van een zaaksofficier van justitie.[34] Deze zaaksofficier draagt de eindverantwoordelijkheid voor het opsporingsonderzoek waarbinnen de hack plaatsvindt en dient daarover dus ook verantwoording af te leggen aan de rechter.

3.3 *Nationale veiligheidsdomein*

De AIVD en de MIVD mogen al langer hacken.[35] De zogeheten 'Joint Sigint Cyber Unit', kortweg 'JSCU', voert zulke operaties uit. Dat is een gezamenlijke uitvoeringseenheid van beide diensten. Een operatie begint met een vooronderzoek om de benodigde capaciteit en de technische

20 *Kamerstukken II* 2022/23, 36263, nr. 3, p. 1. Zie ook AIVD, MIVD & NCTV, *Dreigingsbeeld Statelijke Actoren 2*, Den Haag 2022, p. 13.
21 Formulering naar artikel 138ab lid 1 Sr en artikel 45 lid 1 sub b Wiv 2017. Vgl. *Kamerstukken II* 2016/17, 34588, nr. 3, p. 77-79; PG-HR 2022, p. 7 en 21; WODC 2022, p. 15-17.
22 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 34; *Kamerstukken II* 2016/17 34 372, nr. 6, p. 9.
23 Artikel 80sexies Sr. De Wiv 2017 sluit nadrukkelijk bij die strafrechtelijke definitie aan: *Kamerstukken II* 2016/17, 34588, nr. 3, p. 76; *Kamerstukken II* 2016/17, 34588, nr. 18, p. 69. Vgl. artikel 1 onder a Cybercrime Verdrag. Zie ook J.W. van den Hurk, 'Geautomatiseerde werken en gegevensdragers, tijd voor vernieuwing', *AA* 2022, afl. 5, p. 363-378.
24 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 85-86.
25 ECW 2021, p. 89.
26 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 77; *Kamerstukken II* 2022/23, 36263, nr. 3, p. 14-15. Vgl. Bijlage II bij CTIVD 2020, p. 10.
27 Zie o.a. WODC 2022, hoofdstuk 3; PG-HR 2022, p. 38-40.
28 Artikelen 126nba, 126uba en 126zpa Sv; *Kamerstukken II* 2015/16, 34382, nr. 3, p. 15-19.
29 PG-HR 2022, p. 27. Bepaalde aanverwante verrichtingen die het binnendringen ondersteunen of mogelijk maken zullen eventueel gebaseerd kunnen worden op artikel 3 Politiewet. Zie PG-HR 2022, p. 42.
30 J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, afl. 8, p. 888-908; J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017, afl. 4, p. 350-359, aldaar p. 355.
31 Zie hoofdstuk 7 van het Besluit onderzoek in een geautomatiseerd werk (*Stb.* 2018, 340). Vgl. PG-HR 2022, p. 21-24 en WODC 2022, p. 41-43 met nadere verwijzingen aldaar.
32 Zie ook Inspectie Justitie en Veiligheid, *Toetsingskader hackbevoegdheid politie* 2022 (online); PG-HR 2022, p. 35-38.
33 *Stb.* 2015, 223.
34 PG-HR 2022, p.
35 Artikel 24 Wiv 2002. Vgl. *Kamerstukken II* 1997/98, 25877, nr. 3, p. 39-40.

haalbaarheid (de slagingskans) in te schatten.[36] Met de benodigde toestemmingen – daarover zo meer – kan het binnendringen beginnen. Eenmaal binnen, hebben de diensten, net als de politie, enkele 'inherente' bevoegdheden. Het betreft (a) het doorbreken van enige beveiliging, (b) het aanbrengen van voorzieningen om versleuteling van gegevens ongedaan te maken, (c) het aanbrengen van voorzieningen om een target te observeren of af te luisteren of (d) het overnemen van gegevens.[37]

In de Wiv 2017 is een aantal al langer gangbare operationele praktijken geëxpliciteerd en ingekaderd. Zo mogen de diensten via de computer van een derde 'doorstappen' naar een *target* en is 'verkennen' als bevoegdheid verzelfstandigd.[38] Tot slot mogen de diensten in bepaalde gevallen geautomatiseerde werken bijschrijven op een al goedgekeurde toestemmingsaanvraag, zodat zij snel kunnen meebewegen als een *target* plots overstapt op een nieuwe server of telefoon.[39]

De verscheidenheid aan hackactiviteiten is groot, misschien wel te groot voor de mal van één wettelijke bepaling. Het kan gaan om kleine acties met een beperkte operationele opbrengst, maar ook om grootschalige operaties die juist veel gegevens opleveren. Zo kunnen de diensten bulkdatasets verwerven, bijvoorbeeld bij een telecomprovider in het buitenland. Dat is een gegevensverzameling waarvan het merendeel van de gegevens betrekking heeft op personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden.[40] Op voorhand is dikwijls al duidelijk dat die bulkdatasets veel gegevens bevatten die niet relevant zijn voor de diensten.[41] Toch kan het verwerven ervan noodzakelijk en waardevol zijn, zo erkennen ook de toezichthouders, voor het tijdig onderkennen en identificeren van dreigingen.[42]

4. Autorisatie

4.1 *Opsporingsdomein*

Chronologisch steekt de autorisatiefase als volgt in elkaar. Het startschot voor een hackoperatie is een projectvoorstel van een tactisch (recherche)team.[43] Vervolgens stelt dat team een haalbaarheidsonderzoek op.[44] De officier van justitie gebruikt de resultaten ervan om binnen het Openbaar Ministerie goedkeuring krijgen voor de hackoperatie. De voorgenomen inzet wordt eerst voorgelegd aan de Centrale Toetsingscommissie (CTC), die voorgenomen inzet toetst op juridische haalbaarheid, mogelijke afbreukrisico's en effectiviteit, en vervolgens aan het College van Procureurs-Generaal.[45] Uiteindelijk is een machtiging van de rechter-commissaris nodig. Die machtiging geldt voor vier weken, maar kan daarna telkens met eenzelfde periode worden verlengd.[46]

De rechter-commissaris verricht een puur juridische toets. De precieze methode van binnendringen hoeft géén onderdeel uit te maken van het bevel en dus ook niet van de machtiging.[47] Zij hoeft zelfs niet per se aan bod te komen bij de CTC.[48] Volgens de wetgever zou een toets op (al te) technische gronden namelijk de opsporingsdiensten nodeloos beperken in de wijze waarop zij uitvoering aan geven het bevel, leiden tot extra werklast voor de rechterlijke macht en voorbijgaan aan het feit dat het doorbreken of omzeilen van de beveiliging van het geautomatiseerde werk flexibiliteit vereist van het technische team. En bovendien: eenmaal prijsgegeven methoden kunnen niet zomaar nog eens worden ingezet.[49] Hierna zal nog blijken, dat dit alles een opmerkelijk contrast vormt met de opvattingen van de toetsingsinstantie voor de diensten.

Dan nu de toepassingspraktijk. De zaaksofficier neemt weleens (telefonisch) contact op met de rechter-commissaris, of andersom, om extra informatie over de hackoperatie uit te wisselen. De rechter-commissaris hoeft geen cyberspecialist te zijn. In principe kan elke rechter-commissaris die zich bezighoudt met zwaardere zaken te maken krijgen met een hackoperatie.

Digit-OM versterkt dan actief informatie over de te verrichten onderzoekshandelingen en de wijze waarop die worden uitgevoerd. Als uitgangspunt geldt dat de Digit-werkwijze op punten afscherming behoeft en dat de rechter dus zal moeten vertrouwen op de kennis, de expertise en de professionaliteit van anderen. De rechter-commissaris verbindt soms wel voorwaarden aan de machtiging, maar lang niet altijd. Tot op heden was er in elk geval geen reden om de machtiging definitief niet te verstrekken.[50]

In het toestemmingstraject blijkt Digit-OM de belangrijkste rol te spelen voor wat betreft de technische aspecten van het hacken.[51] Het treedt op als vraagbaak en adviseur

36 CTIVD 2017, p. 13.
37 Artikel 45 lid 2 Wiv 2017. Vgl. Bijlage II bij CTIVD 2020, p. 7.
38 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 75-82. Vgl. ECW 2021, p. 87-88.
39 Het moet dan gaan om een geautomatiseerd werk dat behoort tot hetzelfde target of derde. Zie Artikel 45 lid 8 Wiv 2017 en ECW 2021, p. 93-94.
40 Zie ECW 2021, p. 42-49. Vgl. *Kamerstukken II* 2022/23, 36263, nr. 3, p. 8-9.
41 Conform artikel 27 Wiv 2017 moeten de diensten bulkdatasets zo spoedig mogelijk op relevantie beoordelen en niet-relevante gegevens verwijderen. Over de vraag op welk abstractieniveau die relevantiebeoordeling moet plaatsvinden is een patstelling ontstaan tussen de diensten en de CTIVD. Zie ECW 2021, p. 57-58. Vgl. R.H.T. Jansen, 'Toezicht onder de Wet op de inlichtingen- en veiligheidsdiensten 2017: een tour de force', *NTM/NJCM-Bulletin* 2021, afl. 4, p. 419-443, aldaar p. 437-438.
42 CTIVD 2020, p. 9; ECW 2021, p. 43-44.
43 PG-HR 2022, p. 31.
44 Zie PG-HR 2022, p. 31 en WODC 2022, p. 72-73.
45 Zie *Kamerstukken II* 2015/16, 34372, nr. 3, p. 38.
46 Artikel 126nba lid 3 en lid 4 Sv.
47 WODC 2022, p. 80.
48 Indien nodig geven de Digit-officier en de Digit-politie een toelichting op het haalbaarheidsonderzoek. Daarin kan ook de technische uitvoering aan bod komen, maar, zo merkt het WODC op, 'over de technische componenten "laat het CTC zich niet erg uit"'. Zie WODC 2022, p. 77-78 en 84.
49 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 103. Vgl. PG-HR 2022, p. 34.
50 WODC 2022, p. 79-82.
51 WODC 2022, p. 170.

voor alle actoren, heeft een rol bij selectie van inzetten, ondersteunt het tactisch team bij het opstellen van een aanvraag én geeft op verzoek of op eigen initiatief toelichtingen aan de CTC en de rechter-commissaris. De technische details van een inzet zullen maar zelden worden voorgelegd aan de zittingsrechter.[52]

4.2 *Nationale veiligheidsdomein*

Bij de diensten is – vooralsnog – de autorisatie van zowel het verkennen als het binnendringen op het allerhoogste politiek-bestuurlijke niveau belegd.[53] Nadat een aanvraag voor een bevoegdhedeninzet (een 'last') door interne juristen is beoordeeld, moet eerst het diensthoofd en dan de minister een fiat geven. Vervolgens beoordeelt de Toetsingscommissie Inzet Bevoegdheden (TIB) de toestemming op rechtmatigheid.[54] Dat oordeel is bindend. Als de TIB een last afkeurt, mag de geplande inzet niet doorgaan. Is de toestemming verleend, dan start de operatie en mogelijk ook het *ex durante*-rechtmatigheidstoezicht door de CTIVD. De toestemming geldt voor drie maanden en mag bij een langer lopende hackoperatie worden hernieuwd, via dezelfde procedure.

Waar zich in de autorisatiefase van een politiehack betrekkelijk weinig buitenstaanders bezighouden met de technische finesses, is dat bij hackoperaties van de AIVD en de MIVD anders. De TIB lijkt zich in de praktijk tamelijk intensief te bemoeien met de hackmethode(s). Dat heeft geleid tot spanningen in de verhouding met de diensten.[55] De crux zit, zo menen wij, enerzijds in de huidige institutionele structuur en anderzijds in de vigerende toetsingswijze.

De TIB bestaat uit drie leden. Twee daarvan moeten rechterlijke ervaring hebben. Het derde lid mag een rechter zijn, maar dat hoeft niet. Er zijn evenzoveel plaatsvervangers. Tot op heden is als (plaatsvervangend) 'technisch lid' steeds een persoon benoemd met een achtergrond in de ICT. Vanuit de gedachte dat een ICT'er cyberoperaties beter kan doorgronden dan de gemiddelde jurist, is die keuze begrijpelijk. Het risico daarvan is echter dat zo iemand operationeel gaat meedenken met (of zelfs: denken voor) de diensten. Volgens de wetgever mag dat derde lid ook een persoon met inzicht in veiligheidsrisico's of deskundigheid op strategisch vlak zijn.[56] Wij vermoeden dat in dat scenario de kans op al te intensieve operationele bemoeiing afneemt.

Dan de toetsingswijze. De TIB-toets is uit de aard der zaak statisch. Dat verhoudt zich echter slecht met het dynamische karakter van een hackoperatie. Het punt is: de diensten kunnen in dit stadium op basis van ervaringsleer wel een en ander schetsen, maar nog niet volledig uittekenen wat de exacte werkwijze gaat zijn in een specifieke situatie. De TIB-toets is bovendien breed. Dat is in zoverre begrijpelijk, dat de wetgever ook een volle toets op noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid wenst.[57] In de praktijk blijkt de toets echter wel erg breed – naar de smaak van de Commissie-Jones-Bos té breed – te worden ingevuld.[58] Zo kijkt de TIB bij de toets van het verzamelen van gegevens (verwerving) vaak ook naar wat de diensten met die gegevens gaan doen (verwerking). Anders dan de rechter-commissaris, wil de TIB bovendien meewegen *hoe* het hacken precies zal plaatsvinden en welke risico's daaraan verbonden zijn.[59]

Het gevaar is dat de TIB, in onze woorden, gaat 'micromanagen'.[60] Als de TIB zich gedetailleerd in uitvoeringskwesties mengt, kan dat ertoe leiden dat aanvragen voor hackoperaties wegens onenigheid over technische aspecten worden afgekeurd, vertraging oplopen of worden teruggetrokken. Volgens de diensten leidt dat tot een verlies aan creativiteit, het missen van (tijdelijke) kansen en flexibiliteit binnen het inlichtingenproces ten behoeve van de nationale veiligheid.[61] Wij voegen daar nog een risico aan toe: het vertrek van goede hackers. Dat alles drukt op de inlichtingenposities.

Wat ons betreft hoort de uitvoering, in het bijzonder van complexe hackoperaties, bovendien uit principiële overwegingen te worden overgelaten aan de professionals. De minister kan daarvoor dan de volledige politieke verantwoordelijkheid nemen en daarover ook verantwoording afleggen aan het parlement. De CTIVD hoort het uitvoeringstoezicht uit te oefenen. Zij is daar, anders de TIB, in personele en in materiële zin ook op toegerust. En om het even scherp te stellen: bij een operatie van commando's achter vijandelijke linies bemoeit de militaire toezichthouder zich ook niet met het aantal kogels dat zij meenemen.

Door patstellingen tussen de TIB en de diensten over de wetsuitleg komen hackoperaties volgens de minister inmiddels nog slechts 'hortend en stotend' op gang.[62] De diensten zouden een klein, maar wezenlijk deel van hun onderzoeken niet (meer) kunnen uitvoeren.[63] Opmerkelijk is dat de geschillen lijken te draaien om relatief kleine juridische punten, die wellicht met een meer teleologische benadering – die rekening houdt met de veranderende

52 Ofwel omdat die technische details er niet in alle zaken toe doen ofwel omdat zij afgeschermd dienen te blijven, ook voor de rechter. Zie WODC 2022, p. 170-171.

53 De Commissie-Jones-Bos adviseert om het toestemmingsniveau voor verkennen intern bij de diensten te beleggen, omdat het huidige niveau wel erg hoog is voor een relatief licht instrument dat een zeer beperkte inbreuk op de privacy met zich brengt. Zie ECW 2021, p. 91. De Cyberwet regelt dit. Zie *Kamerstukken II* 2022/23, 36263, nr. 3, p. 14-15.

54 Artikel 32 lid 2 Wiv 2017.

55 Zie uitgebreid ECW 2021, hoofdstuk 9.

56 *Kamerstukken II* 2016/17, 34588, nr. 18, p. 51.

57 *Kamerstukken II* 2016/17, 34588, nr. 18, p. 39.

58 ECW 2021, p. 126-132.

59 ECW 2021, p. 126.

60 Vgl. Jansen 2021, p. 419-443, aldaar p. 431-434.

61 ARK 2021, p. 36-40.

62 *Kamerstukken II* 2022/23, 36263, nr. 9, p. 4.

63 ECW 2021, p. 4; ARK 2021, p. 15-16.

technologische realiteit – zouden kunnen worden opgelost. Een sprekend voorbeeld is de discussie over het bijschrijven van apparaten en daaraan gerelateerde vraag of het begrip 'van' in 'geautomatiseerd werk van' in bijna eigendomsrechtelijke dan wel in wat ruimere zin moet worden uitgelegd. De TIB pleegt 'van' zeer strikt uit te leggen. De diensten vinden die uitleg achterhaald, omdat een infrastructuur tegenwoordig vaak virtueel is en wordt gedeeld door meerdere mensen of organisaties. Zij willen, kortom, ook kunnen overstappen op geautomatiseerde werken die niet uitsluitend door het target worden gebruikt. (Voor de fijnproever: wij refereren hier aan het exclusiviteitsvraagstuk.)[64]

Tot op heden trekt de TIB steeds aan het langste eind. Zij mag nu eenmaal de *go* of *no go* geven. Als de diensten het niet eens zijn met een afwijzing, loopt het spaak. Onder het vigerende regime is er geen andere instantie die mag beoordelen of de TIB-toets op juiste wijze heeft plaatsgevonden, laat staan een heroverweging mag maken. Volgens de Commissie-Jones-Bos is het niet alleen praktisch onwenselijk maar ook principieel niet passend dat de toezichthouder het laatste woord heeft over de uitleg van wettelijke begrippen, de invulling van de toetsingsnormen én de intensiteit van de toetsing. Op haar aanraden wil de wetgever nu dan ook een beroepsprocedure optuigen bij de Afdeling bestuursrechtspraak van de Raad van State.[65] Dat lijkt ons een goede zet.

Wat niet helpt bij het verminderen van de ontstane spanningen in de autorisatiefase, zo denken wij, is dat de procedure bij de TIB volledig schriftelijk verloopt. Waar de rechter-commissaris nog weleens (telefonisch) overlegt met de officier van justitie of soms zelfs in persoon bij een bevoegdhedeninzet door de politie aanwezig is, zit de TIB op afstand. De lijn lijkt ook nog altijd te zijn, zoals voormalig TIB-voorzitter Moussault het eens verwoordde, 'wij onderhandelen niet. Een nieuw verzoek indienen kan wel'.[66] Opvallend is echter dat de TIB regelmatig aanvullende vragen heeft over de voorgenomen operatie (terwijl niet altijd evident is dat die vragen betrekking hebben op rechtmatigheidskwesties) en soms aanvullende voorwaarden oplegt (terwijl de wet niet voorziet in de figuur die de 'geclausuleerde toestemming' is gaan heten).[67] Blijkbaar vormen onduidelijkheden over technische issues voor de TIB een heikel punt bij de *ex ante*-toetsing. Verdiepende gesprekken gericht op wederzijds begrip, eventueel in de vorm van een zitting, zouden dan kunnen helpen.

5. Kwetsbaarheden en technische risico's

5.1 *Algemeen*

Een geautomatiseerd werk kan men binnendringen via een kwetsbaarheid (*bug*). Dat is een zwakke plek in software, dikwijls een programmeerfout, die soms jarenlang onopgemerkt blijft. Een kwetsbaarheid kan meestal worden verholpen met een software-update (*patch*). Zolang die update niet is gemaakt door de producent of niet is geïnstalleerd door de gebruiker, is binnendringen mogelijk.

De variëteit in kwetsbaarheden is groot. Een bekende kwetsbaarheid is een kwetsbaarheid die reeds publiekelijk bekend is, waaronder bij de producent. Er zijn ook onbekende kwetsbaarheden. Tot het moment van bekendmaking spreekt men over een *zero day*. Daarover is het nodige te doen geweest in het parlement.[68] De indruk kan ontstaan dat de politie en de diensten zulke *zero days* op grote schaal gebruiken. Toch is dat niet geval. De meest beruchte *zero days*, die in wijdverbreide hard- en software, zijn ook meteen de meest zeldzame.[69] Als een kwetsbaarheid wel bekend is bij de autoriteiten, maar nog niet bij de producent heet dat een 'bekende onbekende kwetsbaarheid'.

In alle gevallen geldt: vóórdat kan worden binnengedrongen, moet de kwetsbaarheid eerst gebruiksklaar worden gemaakt (*weaponizen* en *exploiten*). De autoriteiten hoeven dat niet altijd zelf te doen. Sterker nog, zij hoeven vaak niet eens zelf te speuren naar (on)bekende kwetsbaarheden. Commerciële partijen en soms ook hackers bieden die namelijk in alle soorten en maten aan.[70]

5.2 *Opsporingsdomein*

De wetgever beschouwt het gebruik van bekende kwetsbaarheden om binnen te dringen als voorkeursoptie. De politie blijkt daar echter maar in een beperkt aantal gevallen gebruik van te maken. Bekende kwetsbaarheden zijn namelijk vooral bruikbaar gebleken voor de niet-telefooninzetten, en die zijn er in veel mindere mate toepast. De politie gebruikt bekende onbekende kwetsbaarheden evenmin snel. Zij wil naar eigen zeggen 'chirurgisch' te werk gaan en daarom geen brede aanval uitvoeren om binnen te dringen. Het binnendringen in een heel specifiek doelwit (een bepaald type geautomatiseerd werk, met een bepaalde versie) vergt echter veel deskundigheid en menskracht. Digit beschikt daar nu niet in voldoende mate over.[71]

Bij bekende onbekende kwetsbaarheden doet zich een ander probleem voor. De wetgever heeft uit politieke overwegingen de verplichting gecreëerd om die netjes te mel-

64 Zie o.a. ECW 2021, p. 93-94; *Kamerstukken II* 2022/23, 36263, nr. 3, p. 18-20; *Kamerstukken II* 2022/23, 36263, nr. 9, p. 53-54 en 68-70.
65 ECW 2021, p. 137-140. Vgl. *Kamerstukken II* 2022/23, 36263, nr. 3, p. 27-39.
66 'De geheime diensten zijn regelmatig niet blij met ons', *NRC Handelsblad* (1 november 2018).
67 ECW 2021, p. 117 en 127-128; ARK 2021, p. 39-40.
68 Denk met name aan het initiatiefvoorstel-Verhoeven Wet zerodays afwegingsproces (vervallen). Zie *Kamerstukken II* 2019/20, 35257.
69 Vgl. ECW 2021, p. 88; *Kamerstukken II* 2022/23, 36263, nr. 3, p. 17.
70 Zie ook N. Perlroth, *This is how they tell me the world ends. The Cyber Weapons Arms Race*, Londen: Bloomsbury Publishing 2021.
71 WODC 2022, p. 94-95.

den bij de producent van de desbetreffende hard- of software.[72] Het idee daarachter is dat die producent vervolgens die kwetsbaarheid zal verhelpen. Dat dient de digitale veiligheid, in brede zin. Op papier ziet de meldplicht er fraai uit, maar in de praktijk blijkt die een knelpunt te zijn. Daar zijn twee redenen voor.

In de eerste plaats differentieert de wet niet in soorten kwetsbaarheden. Alle kwetsbaarheden moeten worden gemeld aan de producent. Naar geldend recht is het weliswaar mogelijk om de bekendmaking van een onbekende kwetsbaarheid uit te stellen, maar niet om die melding achterwege te laten.[73] Periodieke herbeoordeling is nodig. Vroeg of laat zal de politie dus ook kwetsbaarheden moeten melden in systemen die speciaal zijn gemaakt voor personen met criminele intenties.[74] In feite worden criminelen dan geholpen om gaten in hun systemen te dichten. Zoiets is, welbeschouwd, bizar. Het binnendringen van systemen van criminelen is immers geen zuiver hypothetische situatie.[75] Een uitzondering daarvoor is wenselijk, zo erkent inmiddels ook de minister.[76]

In de tweede plaats bemoeilijkt de meldplicht internationale samenwerking. Waar in Nederland een meldplicht geldt, worden kwetsbaarheden in veel andere landen juist als staatsgeheim aangemerkt. Dat wreekt zich: als een partner met de Nederlandse politie wil samenwerken bij een hackoperatie, zal de politie de desbetreffende kwetsbaarheid in principe moeten melden bij de producent – ook al gaat het om een staatsgeheime kwetsbaarheid. ‘Om die reden ziet Digit zichzelf genoodzaakt tegen het buitenland te zeggen dat zij beter hun mond kunnen houden, zodra zij iets willen vertellen over de manier waarop zij een computersysteem willen binnendringen. Dat maakt de samenwerking er niet prettiger op’, zo constateert het WODC droogjes.[77]

5.3 *Nationale veiligheidsdomein*

De diensten gebruiken in veel gevallen een reeds algemeen bekende kwetsbaarheid; het gebruik van een onbekende kwetsbaarheid (zelf ontdekt of aangekocht) komt slechts in beperkte mate voor.[78] Anders dan de politie, beschikken zij wél over een juridische *escape*. Bij onbekende kwetsbaarheden is het uitgangspunt ‘melden, tenzij’.[79] Melding mag achterwege blijven als de nationale veiligheid dat vergt.[80] Aan het niet-melden kunnen wettelijke argumenten (geheimhouding van actuele kennisniveaus, bronbescherming, afscherming van modus operandi) of operationele overwegingen (schade aan lopende operaties of inzet in het kader van een gewapend conflict) ten grondslag liggen. De diensten moeten per casus afwegen of melding mogelijk is. Zij bezien periodiek of niet-gemelde kwetsbaarheden alsnog voor melding in aanmerking komen. De CTIVD ziet daar op toe. Onder het Cyberwetregime zal zij zelfs bindend kunnen oordelen over de inzet van de hackbevoegdheid en in dat kader ook over het gebruik van bepaalde kwetsbaarheden.[81]

In de discussie over hackoperaties van de AIVD en de MIVD gaat veel meer aandacht uit naar een aanpalend thema: de technische risico’s. Men kan die onderverdelen in risico’s die samenhangen met bepaalde kwetsbaarheden en risico’s die ontstaan door handelingen van de diensten zelf. Op dit moment zijn de diensten verplicht beide soorten risico’s te omschrijven in de aanvraag voor een bevoegdhedeninzet.[82] Dat is makkelijker gezegd, dan gedaan. De realiteit is namelijk dat niet alle risico’s op voorhand zijn uit te tekenen. Wij hintten daar al op.

De vraag is vooral hoe gedetailleerd de omschrijving van die risico’s in toestemmingsverzoeken van de diensten zou moeten zijn. De TIB en de diensten verschillen daarover van mening. De TIB wil een goed geïnformeerde rechtmatigheidstoetsing kunnen verrichten en eist tamelijk diepgaand inzicht in de technische risico’s. Dat is tot op zekere hoogte natuurlijk begrijpelijk, omdat de TIB voor de proportionaliteitsafweging zicht zal willen krijgen op eventuele nevenschade. Maar de TIB lijkt er wel wat ver in te gaan. Zij blijkt ook dit vereiste breed te interpreteren en vraagt regelmatig gedetailleerde informatie op over technische risico’s die verder strekt dan hetgeen noodzakelijk is voor een afweging van proportionaliteit, subsidiariteit, noodzakelijkheid en gerichtheid.[83]

De diensten vinden de huidige situatie onwerkbaar. Volgens hen is het niet mogelijk om vooraf alle risico’s te identificeren. Er is op voorhand nu eenmaal, zo signaleerden wij hier ook al, geen volledige blauwdruk beschikbaar van de technische omgeving van een doelwit. Om obstakels bij de TIB-toets te voorkomen, zien de diensten zich gedwongen om uitvoerig allerhande risico’s uit te diepen. Dat heeft tot een toename van de administratieve lasten geleid. In de Tweede Kamer verkondigde MIVD-directeur Swillens recent dat toestemmingsaanvragen nu gemiddeld tien tot dertig pagina’s beslaan, met uitschieters voor

72 Artikel 126ffa Sv.
73 Artikel 126ffa Sv.
74 Op voet van artikel 126ffa Sv kan de officier wegens een ‘zwaarwegend opsporingsbelang’ wel uitstel bevelen; de rechter-commissaris moet dat uitstel periodiek toetsen. Zie WODC 2022, p. 15-16 en 96-97; PG-HR 2022, p. 46-48.
75 WODC 2022, p. 97.
76 *Kamerstukken II* 2023/24, 34372, nr. 31, p. 6.
77 WODC 2022, p. 97.
78 CTIVD 2017, p. 26.
79 Beleid AIVD en MIVD over omgang met onbekende kwetsbaarheden 2018 (online raadpleegbaar). Eerder had de regering in reactie op een Eerste Kamermotie al toegezegd belangendragers te informeren over onbekende kwetsbaarheden, tenzij wettelijke argumenten of operationele redenen daaraan in de weg stonden. Zie *Kamerstukken I* 2014/15, CVIII, O.
80 Dat komt overeen met het *responsible disclosure*-beleid van het Nationaal Cyber Security Centrum.
81 *Kamerstukken II* 2022/23, 36263, nr. 3, p. 17-18.
82 Artikel 45 lid 3 sub a jo. artikel 29 lid 2 Wiv 2017.
83 ECW 2021, p. 92.

hackoperaties tot meer dan zeventig pagina's.[84] Eerder heeft ook de Algemene Rekenkamer al gesignaleerd dat de doorlooptijden zijn toegenomen.[85]

Via de Cyberwet wil de regering de detailvragen over technische risico's aan banden te leggen.[86] De toetsing van die risico's zal evenwel niet geheel verdwijnen. Onder het voorgestelde regime mag (en moet) de TIB alle risico's die op het moment van de aanvraag bekend zijn betrekken in haar proportionaliteitstoets. De diensten zullen zich voortaan echter mogen beperken tot de 'voorzienbare' risico's. Ter compensatie van deze verhoging van het abstractieniveau van de toetsing zal er bindend toezicht van de CTIVD komen op de uitvoering, waaronder op de technische risico's.[87] Dat lijkt ons een zinnige verschuiving van het zwaartepunt in het toezicht.

6. Technische hulpmiddelen en diensten

6.1 *Opsporingsdomein*

In het verlengde van het voorgaande ligt de vraag of de autoriteiten gebruik mogen maken van commerciële producten, meer in het bijzonder van *intrusion software* of *spyware*.[88] Dit speelt in beide domeinen. De politie mag hacksoftware inzetten, maar onder strikte voorwaarden. De wetgever ziet commerciële software als 'uiterste' optie, bijvoorbeeld voor gevallen waarin *social engineering* of bepaalde kwetsbaarheden tekortschieten. Er is namelijk een groot nadeel: de samenstelling en de werking van het commerciële product is voor Digit een *black box*, omdat die informatie behoort tot het bedrijfsgeheim van de producent.[89]

Zulke hacksoftware maakt vrijwel altijd gebruik van onbekende kwetsbaarheden. Welke precies, is doorgaans bedrijfsgeheim en weet Digit dus niet.[90] Op dergelijke producten is de meldplicht dan ook niet van toepassing. Wel wordt binnen het Openbaar Ministerie getoetst of het gebruik van de software in een concrete casus noodzakelijk is. Ook zal screening van een potentiële leveranciers plaatsvinden door de AIVD. Bovendien mogen de leveranciers geen diensten verlenen aan 'dubieuze regimes'.[91]

De wetgever ziet liever dat de politie zélf methoden ontwikkelt om geautomatiseerde werken binnen te dringen. Daar zijn ook extra financiële middelen voor vrijgemaakt.[92] Toch blijkt dat de politie in het overgrote deel van haar inzetten commerciële software en hackdiensten gebruikt.[93] Dat heeft verschillende redenen. Eerst en vooral: het vinden van onbekende kwetsbaarheden in veelgebruikte geautomatiseerde werken is lastig en tijdrovend.[94] Dat geldt zeker voor kwetsbaarheden in mobiele telefoons. Al zou zij dit zelf misschien graag anders zien, de politie beschikt niet in voldoende mate over de daarvoor benodigde kennis en kunde. En als de politie wél een kwetsbaarheid vindt, zal zij die moeten melden bij de producent. De gedachte dat de politie zelf een kwetsbaarheid vindt en benut vraagt grote investeringen voor eenmalig gebruik en is dus niet realistisch.

Voor het aankopen van software is een drempel opgeworpen in het regeerakkoord van kabinet-Rutte III. De politie moet per zaak een licentie aanschaffen.[95] De 'ratio' hierachter is dat de overheid de handel in kwetsbaarheden op geen enkele manier mag stimuleren. Dit lijkt echter averechts uit te pakken. Omdat voor veel inzetten een commercieel product essentieel is, en de politie dus telkens een nieuwe licentie moet aanschaffen, loopt het totaal van de aankoopsommen op tot 'enkele miljoenen'.[96] Het voorgeschreven licentiemodel leidt, kortom, tot extra kosten voor de politie en daarmee tot een extra, onbedoelde beloning en stimulans voor deze markt.[97] De minister heeft recent dan ook een beleidswijziging aangekondigd: eenmaal aangeschafte software mag voortaan worden hergebruikt.[98]

Met binnendringingssoftware is men er meestal nog niet. Idealiter wordt vervolgens een technisch hulpmiddel ingezet, om onderzoekshandelingen te verrichten op het geautomatiseerde werk.[99] In de afgelopen twee jaar heeft Digit hulpmiddelen ontwikkeld, waarmee relevante data kunnen worden opgehaald bij de verdachte. Het gaat dan bijvoorbeeld om chatberichten, e-mails, geluidsbestanden. Om de integriteit van dat materiaal voor een eventu-

84 Technische briefing door de AIVD en de MIVD over de Tijdelijke wet cyberoperaties. De briefing is niet uitgeschreven, maar terugkijkbaar via https://debatgemist.tweedekamer.nl/node/31298. Zie vanaf min 15:20.

85 ARK 2021, m.n. hoofdstuk 4. Vgl. *AIVD/MIVD 2018-2023. Verslag van het functioneren van de diensten*, Den Haag 2023, p. 6.

86 Artikel 5 Conceptvoorstel Cyberwet.

87 Vgl. *Kamerstukken II* 2022/23, 36263, nr. 3, p. 15-17.

88 Zie WODC 2022, p. 101-104. Vgl. P.H.P.H.M.C. van Kempen, 'Spyware – over duidelijke strafwetgeving, de rechtsgoedtheorie en een geconcentreerde regeling', *DD* 2021, afl. 9, p. 789-805; L. Riecke, 'Unmasking the Term "Dual Use" in EU Spyware Export Control', *The European Journal of International Law* 2023, afl. 3, p. 697-719.

89 *Kamerstukken II* 2018/19, 34372, nr. 29, p. 10. Vgl. PG-HR 2022, p. 44; WODC 2022, p. 173.

90 WODC 2022, p. 99-100. De politie heeft procedurele afspraken gemaakt met de leverancier over toegangsrestricties, maar kan die niet afdwingen. Zie Inspectie 2023, p. 19.

91 Dat wil zeggen: aan landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht. Zie *Handelingen I* 2017/18, nr. 34, 5, p. 29. Vgl. PG HR 2022, p. 43-46; WODC 2022, p. 103-104.

92 *Kamerstukken II* 2018/19, 34372, 29 p. 9.

93 PG-HR 2022, p. 114-115; WODC 2022, p. 173; Inspectie 2023, p. 10-11.

94 WODC 2022, p. 173.

95 *Vertrouwen in de toekomst* (coalitieakkoord 2017-2021; VVD, D66, CDA en CU), p. 3.

96 De precieze bedragen zijn geheim. Zie WODC 2022, p. 104-105 en 173.

97 Vgl. Inspectie 2023, p. 20.

98 *Kamerstukken II* 2023/24, 34372, nr. 31, p. 5-6 en 15-17.

99 Zo past het product beter in de context van de Nederlandse wetgeving, waarin een onderscheid bestaat tussen binnendringen en onderzoekshandelingen. Zie WODC 2022, p. 101.

ele strafzaak te verzekeren, kan Digit met die tools de verzamelde data versleuteld opslaan, hashen en digitaal ondertekenen.[100]

De wetgever heeft nog een extra waarborg opgetuigd. Voorafgaand aan de inzet dient een technisch hulpmiddel in beginsel te worden gekeurd door een onderdeel van de Landelijke Eenheid van de Nationale Politie: de Keuringsdienst.[101] Dat is internationaal uitzonderlijk.[102] Deze keuringsinstantie moet aan de hand van een protocol 'objectief en onafhankelijk' beoordelen of het hulpmiddel voldoet aan de wettelijke eisen. Bijzondere aandacht gaat daarbij uit naar de detectie, de registratie en het transport van gegevens. De keuring vindt 'proefondervindelijk' plaats en neemt enkele maanden in beslag.[103]

De keuring is in de praktijk een hinderpaal. Samengevat: de Keuringsdienst eist dat het hulpmiddel altijd aan alle regels uit het Bogw voldoet, ongeacht uitvoeringsconsequenties, terwijl Digit wenst dat aandacht uitgaat naar bewijswaardes en risicoanalyses. In dat laatste perspectief is het niet per se problematisch als een hulpmiddel niet volledig is goedgekeurd, omdat men er in de rechtszaal altijd nog verantwoording over kan afleggen.[104]

Vorig jaar is in het gros van de gevallen een commercieel hulpmiddel ingezet dat niet is gekeurd. Dat is inmiddels een trend, want ook in voorgaande jaren hadden de meeste hulpmiddelen de keuring (nog) niet doorstaan.[105] Dit probleem in de uitvoeringspraktijk betreft een specifieke, maar veelvoorkomende categorie inzetten: onderzoekshandelingen op mobiele telefoons.[106] Deze nieuwe 'standaardpraktijk' is duidelijk niet in lijn is met het wettelijke uitgangspunt.

6.2 *Nationale veiligheidsdomein*

Over de inzet van hacksoftware door inlichtingen- en veiligheidsdiensten is de laatste tijd veel te doen. De Pegasus-onthullingen zijn daarvoor de aanleiding. Heel kort: recent kwam aan het licht dat de diensten van onder andere Polen en Hongarije *spyware* van het Israëlische bedrijf NSO Group hadden ingezet tegen opposanten van de regering. Naar aanleiding van die onthullingen heeft een enquêtecommissie van het Europees Parlement onderzoek verricht naar *spyware*. In haar rapport stelt de enquêtecommissie onder meer dat het misbruik van commerciële software aan banden moet worden gelegd – over een verbod rept zij niet – en dat er een speciale taskforce moet komen ter bescherming van een dergelijke inmenging in democratische processen. Effectief toezicht op de inzet van *spyware* acht zij daarvoor cruciaal.[107] Tweede Kamerlid Pieter Omtzigt bracht even later, als rapporteur van de Raad van Europa, een rapport met soortgelijke conclusies uit.[108]

Of de Nederlandse diensten gebruikmaken van Pegasus, is nooit officieel bevestigd.[109] De minister heeft onderstreept dat het wettelijk niet toegestaan is om in het openbaar inzicht te geven in (uitgaven die verband houden met) de *modus operandi* van de AIVD en de MIVD. De bewindsvrouw merkte wel op dat de diensten onder strikte voorwaarden mogen hacken ter bescherming van de nationale veiligheid en dat de TIB en de CTIVD daarop toezien.[110] Naar geldend recht mag daarbij gebruik worden gemaakt van software – zelfgebouwd of aangekocht.[111]

De politie heeft, als gezegd, vooral binnengedrongen in mobiele telefoons.[112] De diensten doen dat ook wel, maar veel van hun hackwerk is specialistischer van aard. Targets maken immers dikwijls gebruik van zeer geavanceerde geautomatiseerde werken en complexe infrastructuren. Maatwerk is dan vereist. Zo heeft de MIVD via een hackoperatie, waarbij een bulkdataset werd verworven, locatiegegevens weten te achterhalen van bij terreurgroep IS aangesloten personen in Syrië.[113] Het is juridisch niet uitgesloten dat de diensten zélf software bouwen voor het binnendringen en de onderzoekshandelingen. Anders dan bij de politie, hoeft dat hulpmiddel niet vooraf te worden gekeurd. Wel kan de TIB er vragen over stellen en de bevindingen meewegen in de rechtmatigheidstoetsing van een toestemmingsaanvraag. De CTIVD zal vervolgens op het gebruik ervan toezien.

100 WODC 2022, p. 113-114.
101 Artikel 14 Bogw. In uitzonderingsgevallen kan, wanneer de officier van justitie dat bepaalt, keuring achteraf plaatsvinden. Van die uitzondering zal in de praktijk niet lichtzinnig gebruik worden gemaakt. Zie artikel 15 Bogw en *Stb.* 2018, 340, p. 45. De Keuringsdienst keurt trouwens ook traditionele technische hulpmiddelen als microfoons en bakens.
102 WODC 2023, m.n. p. 91-104.
103 *Stb.* 2018, 340, p. 40-43.
104 WODC 2022, p. 175-176.
105 PG-HR 2022, p. 108-109.
106 Inspectie 2023, p. 11.
107 *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*, Brussel: Europees Parlement 2023, raadpleegbaar via https://emeeting.europarl.europa.eu/emeeting/committee/en/agenda/202305/PEGA?meeting=PEGA-2023-0508_1&session=05-08-19-00.
108 *Pegasus and similar spyware and secret state surveillance*, Staatsburg: Raad van Europa 2023, raadpleegbaar via https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68. Het gebruik ervan zou met name op gespannen voet staan met het EVRM, met de EHRM-jurisprudentie daarover en met het nog in werking te treden Protocol tot wijziging van het Dataprotectieverdrag ('Conventie 108+'). Zie ook CTIVD/TIB, Brief aan de Tweede Kamer der Staten Generaal, d.d. 17 februari 2021 (online) en R.H.T. Jansen & M.D. Reijneveld, 'Conventie 108+ en (toezicht op) gegevensverwerkingen in het nationale veiligheidsdomein', *Computerrecht* 2021/208, afl. 5, p. 411-422.
109 Vgl. EP-Pegasusrapport, randnummers 128-129; 'AIVD gebruikt omstreden Israëlische hacksoftware', *de Volkskrant* (2 juni 2022). Omtzigt noemt in zijn rapport Nederland als een van de lidstaten 'which seem to have acquired or used Pegasus', randnummer 13.
110 *Aanhangsel bij de Handelingen 2021/22*, 3252, p. 2-3.
111 Artikel 45 lid 1 sub b Wiv 2017; *Kamerstukken II* 2016/17, 34588, nr. 3, p. 77-79.
112 WODC 2022, p. 89.
113 Zie o.a. ECW 2021, p. 40; 'Inlichtingendiensten moeten data over miljoenen mensen verwijderen', *RTL Nieuws* (16 juni 2022).

7. Controle en toezicht

7.1 *Opsporingsdomein*

Het toezicht op hacken is zwaarder en intensiever dan op andere bijzondere opsporingsmiddelen, maar wel gefragmenteerd.[114] In hoofdlijnen: het Openbaar Ministerie is op verschillende niveaus en op verschillende momenten (vooraf, tijdens en na afloop) betrokken bij de inzet van de hackbevoegdheid. De Inspectie Justitie en Veiligheid oefent tijdens hacken nalevingstoezicht uit en streeft naar een systeem van 'systeemtoezicht'.[115] Dat toezicht strekt zich uit tot het optreden van de politie, maar niet tot dat van de justitiële autoriteiten.[116] Het handelen van de zaaksofficier kan worden getoetst door de rechter in een strafzaak of door de procureur-generaal bij de Hoge Raad in het kader van zijn in algemene 'toezichttaak' op het Openbaar Ministerie ex artikel 122 Wet op de rechterlijke organisatie.[117] Tot slot ziet de Autoriteit Persoonsgegevens toe op de regels rondom persoonsgegevensbescherming en biedt de Nationale Ombudsman aanvullende rechtsbescherming.[118]

Met name de reikwijdte van het systeemtoezicht door de Inspectie staat ter discussie. Een moeilijk punt is het onderscheid tussen de onderwerpen waarop de Inspectie toezicht houdt en de onderwerpen die voor rekening komen van het Openbaar Ministerie en de procureur-generaal bij de Hoge Raad. Het startschot van deze discussie was een opmerking in een rapport van de Inspectie over de betrouwbaarheid van het verzamelde bewijs. Volgens het Digit-OM zou niet de Inspectie, maar uitsluitend de rechter bevoegd zijn tot het doen van dergelijke uitspraken.[119] Inmiddels lijken de betrokken partijen een *modus vivendi* te hebben gevonden, zij het niet van harte.

Hoewel de Inspectie dat zelf graag anders zou zien, oefent zij tot nu toe vooral 'eerstelijns' toezicht uit, dat randvoorwaardelijk van aard lijkt en de nadruk legt op de naleving van regels. De Inspectie onderzoekt of allerlei operationele zaken op orde zijn, zoals bijvoorbeeld de autorisaties van opsporingsambtenaren en de logging. Dat is, zo constateert het WODC, niet in lijn met hoe 'systeemtoezicht' eruit moet zien. Dat toezicht zou gericht moeten zijn op de vraag of de uitvoering verloopt volgens geldend recht en idealiter worden 'gevoed door een 'kwaliteitssysteem' van de politie waarmee zij haar eigen 'interne controle' organiseert'.[120]

Vanwege 'operationele drukte' heeft de politie moeite om goede werkprocessen op te stellen, met als gevolg dat de door de Inspectie 'benodigde en gevraagde verantwoording in de praktijk wringt met hoe er gewe[r]kt wordt bij de politie'.[121] In haar meest recente rapport beklemtoont de Inspectie andermaal dat de politie nog onvoldoende heeft uitgewerkt hoe zij de logging inricht en toepast. Zo vinden controles door de politie zelf slechts op *ad hoc*-basis plaats, zijn beeldschermopnamen nog niet volledig en kloppen de opgestelde journaals niet altijd. Ook niet onbelangrijk: de beveiliging van informatie zou 'nog steeds niet aantoonbaar op niveau' zijn.[122] Volgens de politie richt de Inspectie zich te sterk op de naleving van regels, zonder daarbij oog te hebben voor uitvoeringskwesties – ook als min of meer vaststaat dat die regels onuitvoerbaar zijn. Het gevolg van dit alles? 'Frictie' met de Inspectie, een 'patstelling' en 'enigszins stroever' wordende verhoudingen op de werkvloer.[123]

Het Openbaar Ministerie is eveneens één à twee dagen per week aanwezig bij de politie. Wekelijks vindt overleg plaats over de stand van zaken met betrekking tot lopende inzetten. Digit-OM vervult tijdens de inzet de rol van aanspreekpunt, vraagbaak en adviseur. Het kijkt mee met inzet en grijpt, indien nodig, in door de spreekwoordelijke 'rode kaart' te trekken. Met de zaaksofficier vindt vooral 'resultaatcontact' plaats over de operationele opbrengst. Daarbij lijken de technische aspecten van de inzet niet zo gedetailleerd aan bod te komen. Het volledig doorgronden van de technische finesses door de officier is 'niet altijd aan de orde' en ook 'niet haalbaar', omdat deze jurist is en in principe niet beschikt over specialistische hackkennis.[124]

7.2 *Nationale veiligheidsdomein*

Het *ex durante*- en *ex post*-toezicht op de AIVD en de MIVD is belegd bij de CTIVD. Tot dusver ligt de nadruk op *ex post*, of preciezer: op diepteonderzoeken. De CTIVD heeft daarvoor ruime onderzoeksbevoegdheden: zij kan staatsgeheime informatie raadplegen, mag zelfstandig de systemen van de diensten doorpluizen en kan medewerkers horen. Een en ander resulteert in rapporten van welhaast wetenschappelijke kwaliteit, voorzien van de nodige ad-

114 In de strafrechtelijke literatuur zijn diverse pleidooien te vinden voor de oprichting van een speciale, onafhankelijke toezichthouder naar het voorbeeld van de CTIVD. Zie m.n. M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht', in: *Handelingen NJV* (2016-1), Deventer: Wolters Kluwer 2016, p. 137-240; Y. Buruma, 'De criminele homo digitalis', *NJB* 2016/1073, afl. 22, p. 1534-1541; M.F.H. Hirsch Ballin & J.J. Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden', *DD* 2023, afl. 1, p. 18-38; R.M. te Molder, M.J. Dubelaar, M.I. Fedorova, S.M.A. Lestrade & T.F. Walree, 'Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing', *Computerrecht* 2023/64, afl. 2, p. 110-117.

115 Artikel 126nba lid 7 Sv. Zie over die vorm van toezicht ook J. Helderman & M.E. Honingh, *Systeemtoezicht. Een onderzoek naar de condities en werking van systeemtoezicht in zes sectoren*, Den Haag: WODC 2009.

116 *Kamerstukken II* 2016/17, 34372, nr. 6, p. 81-83; *Kamerstukken I* 2017/18, 34372, G, p. 2 en 14; *Handelingen I* 2017/18, nr. 34, item 5, p. 19; *Stb.* 2018, 340, p. 23-24.

117 Die toezichttaak strekt zich dus niet uit tot de beslissing van de rechter-commissaris. Zie ook PG-HR 2022, p. 13.

118 *Kamerstukken I* 2016/17, 34372, D.

119 WODC 2022, p. 148-150.

120 WODC 2022, p. 150.

121 WODC 2022, p. 150-151. Terecht acht de minister 'het uitputtend beschrijven van de toepasselijke werkprocessen niet realistisch'. Zie *Kamerstukken II* 2020/21, 29628, nr. 1030, p. 9.

122 Inspectie 2023, p. 20-21.

123 WODC 2022, p. 18, 151-154 en 177. Vgl. PG-HR 2022, p. 122-123.

124 Het WODC ligt toe: 'Een zaaksofficier krijgt alleen informatie over wat Digit nodig acht, mocht een zittingsrechter de zaak inhoudelijk behandelen. In dat opzicht moet de zaaksofficier erop vertrouwen dat Digit het goede doet'. Zie WODC 2022, p. 170-171.

viezen, die de minister in nagenoeg alle gevallen overnemen. Wij refereerden hier al aan twee rapporten over hackoperaties.

Vooralsnog hebben zich bij dat toezicht, voor zover wij weten, geen grote problemen voorgedaan. Wel raakt dit aan een algemener punt: de CTIVD mag wel signaleren en adviseren, maar niet interveniëren. Als het aan de CTIVD ligt, verandert dat op korte termijn. In dit verband rept men ook wel over 'doorzettingsmacht'.[125] *In concreto*: de CTIVD wil een operatie kunnen stilleggen of stopzetten en eventueel het wissen van gegevens afdwingen. Hoewel de Commissie-Jones-Bos zulks heeft ontradenen en in de literatuur is gewaarschuwd voor een 'geformaliseerd conflictmodel',[126] lijkt de regering dit model te hebben omarmd – althans, in de Cyberwet. Als het parlement daarmee instemt, zal de CTIVD voortaan bepaalde bindende oordelen vellen.[127] Die oordelen zullen appellabel zijn bij de Afdeling bestuursrechtspraak van de Raad van State.[128] Rechterlijke tegenmacht lijkt ons belangrijk, al was het maar omdat dergelijk ingrijpen grote operationele impact zal hebben. In een democratische rechtsstaat behoort een rechter daarover het laatste woord te hebben.

De CTIVD streeft voorts naar het uitbouwen van het '*real time*-toezicht'. Daarvoor worden al ICT'ers geworven.[129] Het is echter niet geheel duidelijk wat men onder *real time*-toezicht verstaat en hoe dat in de praktijk precies uitpakt. Zoals wij het begrijpen, komt dat neer op frequenter en meer intensiever toezicht gedurende een operatie, bijvoorbeeld via handmatige of automatische controle van logs. Dat lijkt waarschijnlijk op het systeemtoezicht bij de politie. Gelet op de veranderende aard van *intelligence*-activiteiten en de ruimere beschikbaarheid van (persoons)-gegevens is die wens begrijpelijk. Deze toezichtmodaliteit kent evenwel een potentieel risico, zeker in een domein waarin de toezichthouder niet toeziet op marktpartijen, maar op instituties die exclusieve overheidstaken uitvoeren. De toezichthouder kan te intensief betrokken raken bij operationele aangelegenheden. Dat kan problematisch zijn, zowel voor de verantwoordelijkheidsverdeling – die via de minister en het parlement behoort te verlopen – als voor de onafhankelijkheid van de toezichthouder zelf.

Als de voorgenomen veranderingen in het toezicht er inderdaad komen (de Tweede Kamer heeft onlangs ingestemd met de Cyberwet), dan schept dat aan twee kanten verplichtingen. De diensten dienen ervoor te zorgen dat hun hackoperaties 'toezichtbaar' zijn. Zij moeten hun activiteiten in elk geval heel nauwkeurig loggen, ervoor zorgen dat hun eigen kwaliteitsborging op orde is en toezichtvriendelijke systemen ontwerpen. Bij de politie is dat, als gezegd, niet anders. Als de diensten minder nadruk op de *ex ante*-toetsing willen, betekent dat méér *ex durante*- en *ex post*-toezicht. Zij moeten bovendien accepteren dat de CTIVD mogelijk een hard oordeel velt en desnoods intervenieert in een operatie – al houdt de toezichthouder hopelijk wel oog voor de operationele complexiteit.

De CTIVD zal gepaste afstand tot operationele afwegingsprocessen moeten zien te bewaren. Dat is een precaire balanceeract, waarbij zeker in het begin moet worden afgetast hoe ver zij kan en mag gaan. Hoewel gebruikmaking van de doorzettingsmacht in het kader van de bescherming van grondrechten zeer wel verdedigbaar kan zijn, is het scenario waarin dat niet nodig is verkieslijk. Als het even kan, moeten verschillen van inzicht op een andere manier worden opgelost. Een soort escalatieladder kan dan helpen. Zelf interveniëren door de CTIVD kan juridisch immers noodzakelijk zijn, maar is het als ware de nucleaire optie, die geheid spanningen in het stelsel veroorzaakt en tot politieke commotie leidt. De toezichthouder moet naast rode ook gele kaarten hebben. Zo kan het afdwingen van normconform gedrag ook plaatsvinden door waarschuwingen aan het hackteam, overleggen met dienstmedewerkers ('normoverdragend gesprek') of adviezen aan de wetgever.

8. Slot

Het parlement heeft omwille van algemene maatschappelijke belangen meermaals – in onze ogen terecht – aangedrongen op het niet-ondermijnen van sterke versleuteling. Tegelijkertijd wil men effectieve criminaliteitsbestrijding en effectieve bescherming van de nationale veiligheid. Hacken biedt dan uitkomst, maar is juridisch complex en technisch specialistisch werk. Op dit moment kan deze bevoegdheid niet altijd goed worden ingezet, zo blijkt uit de hier besproken rapporten.

Wij menen bij de wetgever de drang te bespeuren om dit type overheidsoptreden – deels uit onbehagen met de cyberwereld, deels uit politieke scoringsdrift – dicht te willen spijkeren. Dat resulteert in steeds meer gedetailleerde toepassingsvoorwaarden en een verdere uitbreiding van het toezichtstelsel. Het probleem is dat dit alles op weinig doordachte wijze gebeurt. Voor zover wij weten bestaat er in elk geval geen heldere, moderne visie op cyberactiviteiten door overheidsactoren.

Het voorgaande heeft, als wij het goed zien, een zelfversterkend effect. Als de wetgever veel gedetailleerde normen opstelt, heeft een toezichthouder ook veel om aan en op te toetsen. Wij vrezen dat deze juridisering van de uitvoering al gauw leidt tot een zekere rechtlijnigheid of zelfs

125 Brief aan ECW van de CTIVD, d.d. 11 augustus 2020 (online).

126 ECW 2021, p. 120-124; verzamelannotatie van E.J. Dommering in *NJ* 2021/361, met randnummer 22.

127 Artikel 12 Conceptvoorstel Cyberwet.

128 Artikel 13 Conceptvoorstel Cyberwet.

129 In 2016 heeft de CTIVD een ICT-unit ingesteld. In verband met de Cyberwet heeft de CTIVD gevraagd om een uitbreiding van haar personele en materiële capaciteit. De regering heeft inmiddels toegezegd 10 fte extra formatie beschikbaar te stellen. Zie *Kamerstukken II* 2022/23, 36263, nr. 9, p. 103-104.

starheid in het systeem, terwijl open normen en teleologische interpretatie van technologische aspecten juist van groot belang zijn voor de toekomstbestendigheid van regels. Via laatstgenoemde route kan de praktijk immers meebewegen met nieuwe technologische ontwikkelingen, zonder dat politiek Den Haag om de haverklap zelf hoeft in te grijpen.

Volgens ons is een verandering in de *mindset* nodig. Bij hacken geldt: *high-risk-high-gain*. De wetgever en de toezichthouders zullen moeten accepteren dat improvisatie soms nodig is. Want hoezeer men het ook wil, hackoperaties laten zich niet op voorhand helemaal uittekenen. En flauw, maar waar: waar gehackt wordt vallen spaanders. De operationele praktijk vraagt wat ons betreft dan ook om niet al te rigide regelgeving, een meer flexibele interpretatie van regels als de technologische realiteit dat vergt, meer dynamische vormen van toezicht, rolvast handelen door toezichthouders en vertrouwen in de professionaliteit van betrokken hackers.

Voor het opsporingsdomein impliceert dit vooral dat men het hacken niet moet willen 'dichtregelen' met detailregels. Spitsen wij dit toe op het nationale veiligheidsdomein, dan betekent dit met name dat de TIB het abstractieniveau van haar toets mag verhogen en meer mag vertrouwen op het vervolgtoezicht van de CTIVD. Ter compensatie ligt een uitbreiding van het *ex durante*- en *ex post*-toezicht in de rede. Dat past het best bij het moeilijk voorspelbare verloop van hackoperaties. De CTIVD zal vervolgens wel gepaste afstand tot operationele afwegingsprocessen moeten zien te bewaren, om te voorkomen dat de verantwoordelijkheidsrelaties vertroebelen.