Information Law and Policy Lab

PIRs under pressure: op zoek naar een wettelijke grondslag voor terughacken door private incident responspartijen in Nederland.

Amsterdam, juli 2025

Dit beleidspaper is geschreven door Florence van Blokland, Jean Mattijsen, Kimberly van der Laan en Kyra Sekac. Zij hebben dit geschreven als onderdeel van het Glushko & Samuelson Information Law and Policy Lab (ILP Lab) van het Instituut voor Informatierecht (IViR) van de Universiteit van Amsterdam (UvA). Het paper omvat de zienswijze en aanbevelingen van de auteurs.

Bij het ILP Lab ontwikkelen studenten onder toezicht van het IViR op onderzoek gestoelde beleidsoplossingen die fundamentele rechten en vrijheden op het gebied van Europees informatierecht beschermen. Dit beleidspaper is tot stand gekomen in samenwerking met Cyberveilig Nederland. Wij danken Ot van Daalen (IViR) voor zijn uitgebreide begeleiding van dit onderzoek, Liesbeth Holterman (Cyberveilig Nederland) en Rosalie Brand (Kennedy Van der Laan) voor hun input.

Inhoudsopgave

Inleiding

Aanpak van ransomware in Nederland

Ransomware is de afgelopen jaren uitgegroeid tot een maatschappelijk ontwrichtende en lucratieve vorm van cybercriminaliteit. Criminelen versleutelen of stelen gegevens van organisaties en eisen losgeld om de toegang te herstellen of te voorkomen dat gestolen data wordt gepubliceerd. Dit leidt niet alleen tot financiële schade, maar ook tot operationele verstoringen en reputatieverlies. Met aanvallen op zowel private als publieke instellingen is de impact aanzienlijk, waarbij de schade in sommige gevallen kan oplopen tot miljoenen euro's.

Om Nederland beter te beschermen tegen ransomware-aanvallen is Project Melissa opgericht. Dit initiatief heeft als doel de digitale weerbaarheid van Nederlandse ondernemingen en instellingen te vergroten en Nederland zelf minder aantrekkelijk te maken voor cybercriminelen. Het project richt zich op het versterken van preventie, het verbeteren van responsstrategieën en het ontwikkelen van een juridisch kader dat samenwerking tussen publieke en private partijen faciliteert.

Project Melissa is een samenwerking tussen het Openbaar Ministerie (OM), het cybercrime-team van de politie, het Nationaal Cyber Security Centrum (NCSC), Cyberveilig Nederland en diverse private cybersecuritybedrijven. De meeste private partijen zijn al aangesloten bij Cyberveilig Nederland, een belangenvereniging die de digitale veiligheid in Nederland bevordert. De sector is onderverdeeld in vier kerngebieden: preventie (het voorkomen van cyberaanvallen), detectie (het tijdig identificeren van bedreigingen), respons (het effectief reageren op incidenten) en governance (het bevorderen van structurele cyberveiligheid binnen organisaties).

De nauwe samenwerking tussen publieke instanties en private partijen binnen Project Melissa moet leiden tot een krachtigere aanpak van ransomware en een structurele versterking van de cyberveiligheid in Nederland.

In het kader van de samenwerking binnen Project Melissa komen diverse vraagstukken ten aanzien van ransomwarebestrijding aan bod. Eén daarvan is de juridische reikwijdte van de bevoegdheden van private partijen in het kader van de responsstap, specifiek: of private partijen zich toegang mogen verschaffen tot

de infrastructuur van aanvallers indien die gelegenheid zich voordoet. Dit onderzoek demonstreert dat er hier geen juridische ruimte voor is op basis van het huidige strafrechtelijke en bestuursrechtelijke kader en suggereert een aantal mogelijke oplossingsrichtingen.

Capaciteitsgebrek & juridische beperkingen

Momenteel is alleen de politie onder bepaalde omstandigheden bevoegd op afstand heimelijk een computer binnen te dringen (art. 126nba, 126uba, 126zpa Sv). Zij speelt daarmee een centrale rol bij het bestrijden van ransomware-aanvallen. Maar voordat de politie wordt ingeschakeld, is er een korte periode waarin verdere slachtoffers kunnen worden voorkomen. In de praktijk schakelen bedrijven en andere slachtoffers van ransomware vaak eerst een PIR-partij in om de aanval te analyseren en te mitigeren. Afhankelijk van de situatie wordt daarna wel of niet de politie betrokken. Het inschakelen van de politie kost namelijk tijd, terwijl private incident response-partijen (PIR-partijen) sneller kunnen handelen.

Wanneer een slachtoffer een PIR-partij inschakelt om het probleem op te lossen, voert laatstgenoemde onderzoek uit naar de aanval. Een exfiltratieserver, waarop gestolen data worden opgeslagen, vormt daarbij vaak een essentieel onderdeel van dat onderzoek. Op die servers worden regelmatig activiteiten gesignaleerd die aantonen dat gelijktijdig een hack bij een derde bedrijf plaatsvindt. Die informatie kan worden gebruikt om derden te waarschuwen en verdere schade te voorkomen - één van de meest effectieve manieren om een hack te laten 'mislukken', zo blijkt uit gevoerde interviews. Daarnaast vinden PIR-partijen vaak de data van het oorspronkelijke slachtoffer, waarvan het belang van het terughalen groot kan zijn als hackers de back-ups hebben weten te beschadigen.

Maar door de strikte bewoording van het strafrecht zouden PIR-partijen al strafbaar kunnen zijn zodra zij een exfiltratieserver betreden of gebruiken om toekomstige slachtoffers te behoeden. Dit brengt hen in een juridisch onzekere positie en kan er uiteindelijk toe leiden dat meer slachtoffers vallen dan noodzakelijk, omdat PIR-partijen uit voorzorg afzien van verder onderzoek, of dit onderzoek slechts in het geheim kunnen uitvoeren. Om zowel bestaande als potentiële slachtoffers beter te beschermen, is er binnen Project Melissa behoefte aan een duidelijker begrip van de juridische kaders waarbinnen PIR-partijen mogen opereren.

Vraagstelling

Hoofdvraag:

Onder welke omstandigheden is het juridisch verdedigbaar dat private partijen in het kader van een ransomware-aanval: (1) zich ongeautoriseerd toegang verschaffen tot een exfiltratieserver (binnendringen), (2) deze server doorzoeken, (3) daarop aangetroffen gegevens kopiëren en/of veiligstellen, (4) deze gegevens delen met andere (potentieel) getroffen partijen, en/of (5) deze gegevens verstrekken aan opsporingsautoriteiten?

Normatieve vervolgvraag:

Indien het huidige juridische kader onvoldoende ruimte biedt voor deze handelingen, welke wijzigingen in het vervolgingsbeleid van het Openbaar Ministerie dan wel in de relevante wet- en regelgeving zouden noodzakelijk zijn om dergelijke handelingen te kunnen rechtvaardigen of legitimeren?

Leeswijzer

Om de hoofdvraag te beantwoorden, is het onderzoek opgebouwd rond zes juridische en normatieve deelvragen. Deze worden niet één voor één besproken, maar verwerkt in vier thematische hoofdstukken. Elk hoofdstuk behandelt een specifieke kant van het juridische en beleidsmatige vraagstuk:

1. **Strafrechtelijke grenzen** – over de strafbaarstelling van toegang tot exfiltratieservers (art. 138ab Sr), de (on)toepasbaarheid van strafuitsluitingsgronden en het opportuniteitsbeginsel in het kader van het vervolgingsbeleid van het Openbaar Ministerie. *(Subvragen 1–3 en 5)*
2. **Rechtsstatelijke risico's** – over de grondrechtelijke, democratische en toezichtgerelateerde bezwaren bij het privatiseren van hack-backhandelingen. *(Subvragen 1–4)*
3. **Wenselijkheid van private interventie** – over de rol van PIR-partijen bij het beperken van schade, beleidsprioriteiten en de verhouding met publieke opsporing. *(Subvragen 2, 4 en 5)*
4. **Juridische verankering via vergunningenstelsel** – over de vraag of, en onder welke voorwaarden, het wenselijk is om private hackbacks juridisch mogelijk te maken via een vergunningenstelsel. *(Normatieve vervolgvraag)*

Deze vier invalshoeken vormen samen het kader voor de analyse en uiteindelijke beoordeling van de juridische toelaatbaarheid van hack-backhandelingen (hierna ook wel aangehaald als terughacken), en de voorwaarden waaronder die eventueel verdedigbaar zijn.

Middelen en beperkingen

Voor dit onderzoek is gebruikgemaakt van een combinatie van kwalitatief onderzoek, juridisch-normatief onderzoek en literatuuronderzoek. Het doel was om zowel een volledig beeld te krijgen van de verschillende belangen die spelen in deze kwestie, als van de juridische en bestuurskundige kaders die relevant zijn voor het uitvoeren van overheidstaken.

Het empirische deel van het onderzoek bestond uit diepte-interviews. De interviews waren semigestructureerd en zijn aangepast op de specifieke expertise van de geïnterviewden, waardoor ruimte ontstond voor verdieping en het verkennen van verschillende perspectieven. Ter voorbereiding hiervan is achtergrondonderzoek gedaan naar de betrokken publieke en private actoren, hun rollen en belangen. Deze analyse vormde de basis van de voorbereiding op de interviews, naast het contextualiseren van de bevindingen.

Daarnaast is doctrinair juridisch onderzoek verricht naar de grondwettelijke basis voor de samenwerking tussen overheid en private partijen. Dit normatieve onderzoek richtte zich op de interpretatie van rechtsbeginselen en bestaande wet- en regelgeving. Aanvullend is onderzocht hoe binnen het Nederlands bestuursrecht bevoegdheden kunnen worden gedelegeerd of gemandateerd aan private partijen, en welke beperkingen daarbij gelden.

Tot slot is er voor het algemene literatuuronderzoek gebruikgemaakt van academische literatuur over democratische legitimiteit. Dit theoretische kader diende ter onderbouwing van onze analyse over de rol van private partijen met overheidsbevoegdheden. Daarbij is gekeken naar de betrokken publieke en private actoren, hun rollen en belangen. Deze analyse vormde de basis voor de voorbereiding van de interviews, als het kader voor het duiden van de bevindingen.

Dit onderzoek kent enkele afbakeningen van het onderzoek. Ten eerste is ervoor gekozen om het juridisch kader uitsluitend te analyseren binnen het Nederlandse recht. Technische aspecten van internationale cyberaanvallen en de mogelijke strafrechtelijke gevolgen voor PIR-partijen die buitenlandse servers

binnendringen, en daarmee onder een ander rechtsstelsel vallen, zijn buiten beschouwing gelaten. Internationaal recht wordt behandeld voor zover het invloed uitoefent op het Nederlandse rechtsstelsel. Hoewel de uitkomsten van dit onderzoek niet direct toepasbaar zijn op andere jurisdicties, zijn de onderliggende argumenten ook relevant voor vergelijkbare discussies in het buitenland.

Daarnaast is de privaatrechtelijke aansprakelijkheid van PIR-partijen buiten beschouwing gelaten. Hun optreden kan, met name wanneer dit onbedoeld schade toebrengt aan derden, leiden tot civielrechtelijke claims, zoals vorderingen op grond van onrechtmatige daad. Aangezien dit onderzoek zich uitsluitend richt op hun mogelijke strafrechtelijke aansprakelijkheid, is nader onderzoek naar de civielrechtelijke implicaties van terughackmaatregelen.

Strafrechtelijke wederrechtelijkheid

Strafrechtelijke wederrechtelijkheid

Het volgende deel van het onderzoek richt zich op de strafrechtelijke aansprakelijkheid van de ethische hacker, in het bijzonder op artikel 138ab van het Wetboek van Strafrecht (Sr), dat computervredebreuk strafbaar stelt. Voor dit onderzoek zijn met name lid 1 en lid 2 van belang. Lid 1 bevat de kernbepaling, waarin strafbaar wordt gesteld het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of een deel daarvan. Lid 2 verhoogt de strafmaat wanneer de dader na het binnendringen gegevens overneemt, aftapt of opneemt.

Naar aanleiding van het Cybercrimeverdrag (2001) is het vereiste van **reële beveiliging** vervallen bij de herziening van de Wet computercriminaliteit II. Dit heeft als gevolg dat voor een (ethische) hacker de kans wordt vergroot om onder art. 138ab Sr te vallen, want er is geen minimumdrempel aan beveiliging meer: zelfs als de 'deur' open wordt gelaten, geldt het alsnog als binnendringen. Dit is bevestigd in een arrest van de Hoge Raad: "Daarbij is niet van belang of die opening inherent is aan het systeem of is veroorzaakt door andere 'aanvallers'."[1] Uit de Kamerstukken blijkt dat bewust ruimte is gelaten binnen art. 138ab Sr om ook andere vormen van binnendringen strafbaar te kunnen stellen, zodat de bepaling mee kan evolueren met technologie[2]. Wat hieruit kan worden opgemaakt, is dat een ethische hacker vrijwel meteen aan het binnendringen is.

Omdat sommige hacks, alleen met het doel om kwetsbaarheden bloot te leggen (ethisch hacken), onder omstandigheden het publiek belang kunnen dienen, is er in een beleidsbrief van het OM een stappenplan uitgewerkt, aan de hand waarvan een officier van justitie kan bepalen of er sprake is van ethisch hacken. Er worden hier drie factoren beoordeeld:

1. Is er gehandeld in het kader van een **wezenlijk maatschappelijk belang**;
2. Is er sprake van **proportioneel** handelen (ofwel: ging de verdachte niet verder dan noodzakelijk was om zijn doel te bereiken?);
3. Is er voldaan aan het **subsidiariteitsvereiste** (ofwel: was/waren er geen minder vergaande manier(en) om het door de verdachte beoogde doel te bereiken?).

Echter, later in de beleidsbrief wordt gesteld dat: “het raadzaam is om in ieder geval de volgende zaken niet te doen (don’ts): **gegevens kopiëren, te wijzigen of te verwijderen.”**[3] Dit betekent dat het voor PIR-partijen doorgaans niet mogelijk zal zijn hierop een beroep te doen voor het informeren van andere slachtoffers. Om slachtoffers te beschermen, moeten de hackers namelijk een van deze acties uitvoeren.

Een vonnis van de Rechtbank Oost-Brabant demonstreert hoe deze factoren in de rechtspraak worden toegepast.[4] De verdachte was meerdere keren binnengedrongen op een website waar medische gegevens stonden opgeslagen en deze, weliswaar geanonimiseerd, gekopieerd en geprint. Hij deed dit om een ernstig beveiligingslek aan te tonen. De rechtbank erkende het maatschappelijk belang en vond het eerste binnendringen en printen niet strafbaar. Echter, omdat de verdachte méér gegevens raadpleegde dan nodig (proportionaliteit) en geen serieuze melding deed bij de organisatie vóór hij de media inschakelde (subsidiariteit), werd zijn verdere handelen wél als strafbaar aangemerkt.

Uit onze interviews met experts binnen het Openbaar Ministerie blijkt dat zij het creëren van ruimte voor ethische hackers via jurisprudentie niet als een reële optie beschouwen, onder meer vanwege het gebrek aan actuele rechtspraak. Tegelijkertijd wordt datzelfde gebrek door anderen juist gezien als reden voor meer rechterlijke beoordelingsvrijheid: omdat de bestaande jurisprudentie verouderd is, zou een rechter vandaag de dag mogelijk tot een ander oordeel komen, mede gezien de toegenomen maatschappelijke erkenning van ethisch hacken.

Ook in het internationale kader zijn er weinig aanknopingspunten voor juridische erkenning van verdergaande vormen van ethisch hacken. Het Verdrag inzake cybercriminaliteit, ook wel het Boedapestverdrag, is een verdrag dat door de lidstaten van de Raad van Europa en 22 andere staten is ondertekend. In art. 2 van dit verdrag komen de ondertekenaars overeen onrechtmatige (letterlijk: “without right”) toegang tot een gedeelte van een computer strafbaar te stellen. “Without right” laat ruimte voor lidstaten om in hun eigen rechtstelsel een grondslag op te nemen waardoor bepaalde vormen van hacken, zoals waartoe de politie bevoegd is, toe te staan.[5]

In dit verband is ook de *Paris Call for Trust and Security in Cyberspace* uit 2018 vermeldenswaardig, die door een deel van de ondertekenaars van het Boedapestverdrag is ondertekend. Dit is een niet-bindende verklaring die oproept om een veilige cyberspace te creëren. Nederland is (net als de rest van Europa) een van de ondertekenaars. Het achtste punt in de bijeenkomst staat centraal. Dit punt verbiedt hack-backs

door 'non-state actors' en moedigt ondergetekenden (zoals Nederland) juist aan om maatregelen te nemen die ze voorkomen.[6]

In nationale context is verder in 2019 de Wet Computercriminaliteit III in werking getreden om het strafrecht omtrent computercriminaliteit te actualiseren. Tijdens de bespreking van het wetsvoorstel specificeerde de wetgever nadrukkelijk dat hack-backs als verdediging niet zijn toegestaan. "De eigenaar mag bij de bescherming van een geautomatiseerd werk echter niet zover gaan dat hij een strafbaar feit pleegt. Het wederrechtelijk binnendringen in een geautomatiseerd werk is als computervredebreuk strafbaar gesteld (art. 138ab Sr). Handelingen die zijn aan te merken als «terughacken» zijn derhalve niet toegestaan."[7]

Rechters houden al rekening met de internationale context, en nu zowel het Cyberverdrag als het nieuwe WvSv een restrictievere koers volgen, lijkt ook in de toekomst binnen de rechtspraak weinig ruimte voor een bredere interpretatie.

Overige aanwijzingen dat ethisch hacken strafbaar zal worden gesteld zijn:

- Ethisch hacken wordt niet in de Richtlijn Strafvordering Cybercrime[8] als een **strafverminderende factor** genoemd;
- Het overnemen van gegevens is juist een strafverzwarende omstandigheid onder art. 138ab lid 2 Sr;
- Wanneer gegevens niet worden overgenomen, maar wel gewijzigd of vernietigd, is er sprake van een overtreding in de zin van art. 350a Sr;
- OM heeft een brede vervolgingsbevoegdheid en er kunnen **geen directe rechten** aan de beleidsbrieven worden ontleend;
- Zelfs als het OM kiest om niet te vervolgen, kan hierover een klacht worden ingediend op grond van art. 12 Sv.

Tussenconclusie

De juridische grenzen van ethisch hacken zijn redelijk duidelijk: kopiëren van gegevens lijkt bijna nooit te mogen. Dit leidt tot terughoudendheid bij het melden van lekken, doordat ethische hackers geen vervolging willen riskeren[9]. Verder blijkt uit de bovenstaande analyse dat een ethische hacker vrijwel meteen aan het binnendringen is in de zin van art. 138ab Sr. Om gegevens te kopiëren, wijzigen of verwijderen als

de hacker eenmaal binnen is, zal hoogstwaarschijnlijk niet in lijn zijn met de beginselen van proportionaliteit en subsidiariteit.

Strafuitsluitingsgronden & vervolgingsbeleid OM

Het uitgangspunt in het Nederlandse strafrecht is dat computervredebreuk, waaronder ook het zogenoemde 'terughacken' valt, strafbaar is op grond van artikel 138ab van het Wetboek van Strafrecht. Toch bestaan er situaties waarin een handeling die in beginsel strafbaar is, niet tot straf leidt. Deze uitzonderingen worden **strafuitsluitingsgronden** genoemd en vormen een belangrijk correctiemechanisme binnen het strafrecht.[10] Ze zorgen ervoor dat iemand die bijvoorbeeld handelt uit nood of ter verdediging niet onterecht strafrechtelijk aansprakelijk wordt gehouden. Er wordt daarbij onderscheid gemaakt tussen **rechtvaardigingsgronden**, waarbij de gedraging zelf niet als wederrechtelijk wordt gezien, en **schulduitsluitingsgronden**, waarbij de gedraging onrechtmatig blijft, maar de dader geen straf krijgt omdat hem geen verwijt kan worden gemaakt.

Een aanvullende route, die formeel niet als strafuitsluitingsgrond geldt, maar wel tot het achterwege laten van straf kan leiden, is het **besluit van het Openbaar Ministerie (OM) om niet te vervolgen**. Dat kan op basis van het zogenoemde opportuniteitsbeginsel (art. 167 lid 2 Sv), bijvoorbeeld wanneer vervolging niet in het algemeen belang is. Deze drie benaderingen, rechtvaardiging, schulduitsluiting en niet-vervolging, vormen samen een aanvullend juridisch kader waarbinnen de toelaatbaarheid van terughacken bij ransomware-aanvallen kan worden beoordeeld.

Er zijn zowel **geschreven** als **ongeschreven** strafuitsluitingsgronden.[11] De geschreven gronden zijn opgenomen in Titel III van Boek 1 van het Wetboek van Strafrecht (artikelen 39 t/m 43 Sr). Ongeschreven strafuitsluitingsgronden zijn niet wettelijk vastgelegd, maar wel erkend in de rechtspraak.

Voor dit onderzoek zijn met name de volgende drie strafuitsluitingsgronden relevant: **(1) Noodweer** (*art. 41 lid 1 Sr*): een rechtvaardigingsgrond waarbij sprake is van verdediging tegen een ogenblikkelijke, wederrechtelijke aanranding. De gedraging wordt dan niet als wederrechtelijk aangemerkt. **(2) Noodweerexces** (*art. 41 lid 2 Sr*): een schulduitsluitingsgrond die van toepassing is wanneer de dader handelt vanuit een hevige gemoedsbeweging die is veroorzaakt door de aanranding, waardoor de verdediging de grenzen van proportionaliteit overschrijdt. **(3) Ontbreken van materiële wederrechtelijkheid** (*ongeschreven*):

een door de rechtspraak erkende rechtvaardigingsgrond waarbij de gedraging formeel strafbaar is, maar niet wederrechtelijk wordt geacht, omdat deze strookt met het doel van de overtreden strafbepaling.

Noodweer (art. 41 lid 1 Sr)

Een beroep op noodweer bij terughacken stuit in de praktijk al snel op het vereiste van een **ogenblikkelijke aanranding**. De Hoge Raad stelt dat de aanranding *actueel* en *dreigend* moet zijn: het gevaar moet zich op dat moment daadwerkelijk voordoen.[12] In het geval van een ransomware-aanval is de feitelijke aanval echter vaak reeds voltooid zodra de bestanden zijn versleuteld. Wat resteert, is schade, geen lopende aanranding. Verdediging tegen een reeds beëindigde aanval valt buiten het bereik van artikel 41 Sr.[13]

Ook wanneer wordt betoogd dat de versleuteling van systemen een **voortdurende aanranding** vormt, vergelijkbaar met gijzeling, blijft het juridische kader strikt. Slechts wanneer het gevaar *daadwerkelijk actueel* is en *alleen door direct ingrijpen kan worden afgewend*, zou mogelijk ruimte bestaan voor noodweer. Denk bijvoorbeeld aan een situatie waarin een ziekenhuis door ransomware de controle over beademingsapparatuur verliest en mensenlevens acuut in gevaar zijn.

Zelfs indien aan het vereiste van een ogenblikkelijke aanranding is voldaan, moet daarnaast worden getoetst aan de overige voorwaarden voor een geslaagd beroep op noodweer: **(1) Subsidiariteit**: was terughacken daadwerkelijk de minst ingrijpende manier om het gevaar af te wenden, of hadden ook alternatieven zoals het gebruik van back-ups, het inschakelen van de politie of het isoleren van systemen uitkomst kunnen bieden? **(2) Proportionaliteit**: staat de terughack in verhouding tot de aanval, of veroorzaakt deze mogelijk meer schade dan wordt voorkomen? **(3) Verdedigingswil**: was de handeling daadwerkelijk gericht op verdediging, of speelden ook motieven zoals vergelding of strategisch voordeel een rol?

Noodweerexces (art. 41 lid 2 Sr)

Voor een geslaagd beroep op **noodweerexces** moeten drie cumulatieve voorwaarden worden vervuld: **(1)** er moet sprake zijn van een objectieve noodweersituatie, **(2)** de verdediging moet de grenzen van proportionaliteit hebben overschreden, en **(3)** deze overschrijding moet het **onmiddellijke gevolg** zijn van een **hevige gemoedsbeweging**, zoals paniek, angst of shock. Voor professionele incidentresponseteams ligt een geslaagd beroep op noodweerexces niet voor de hand. Van deze actoren mag immers beheerst en planmatig optreden worden verwacht. Een hevige gemoedsbeweging die zodanig intens is dat zij de gedraging volledig verklaart, wordt in die context al snel als **ongeloofwaardig** aangemerkt.

Ontbreken van materiële wederrechtelijkheid (ongeschreven)

Dit leerstuk houdt in dat een gedraging die formeel onder een delictsomschrijving valt, toch niet strafbaar is, omdat zij materieel gezien niet in strijd is met het recht. Met andere woorden: de handeling schendt weliswaar de letter van de wet, maar strookt met het doel of de strekking ervan. De klassieke toepassing is te vinden in het Huizense veearts-arrest: een dierenarts die in strijd met een wettelijk verbod toch vee vaccineerde om een epidemie te voorkomen, werd niet gestraft omdat hij handelde ter bescherming van een hoger rechtsgoed dan het belang dat door het strafverbod werd beschermd.[14]

Toepassing op het terughacken door private partijen stuit echter op bezwaren. In de kern is het strafbaar stellen van computervredebreuk (art. 138ab Sr) juist bedoeld om ongeautoriseerde toegang tot geautomatiseerde systemen te voorkomen, ongeacht het motief. Terughacken is dan ook geen handeling die het achterliggende rechtsbelang van de norm (digitale integriteit en systeemautonomie) ondersteunt, maar die datzelfde belang schendt. Daarmee lijkt de afwezigheid van materiële wederrechtelijkheid bij terughacken slechts in uitzonderlijke omstandigheden verdedigbaar. Daarnaast geldt dat een belangenafweging over wat het 'hogere doel' is, bij uitstek toekomt aan de wetgever of rechter, niet aan private actoren. Toepassing van dit leerstuk vereist daarom grote terughoudendheid.

Besluit tot niet-vervolging door het Openbaar Ministerie en art. 12 procedure

Op grond van artikel 167, tweede lid, Wetboek van Strafvordering (Sv) kan het Openbaar Ministerie besluiten om van vervolging af te zien indien het daartoe op grond van het **opportuniteitsbeginsel** aanleiding ziet. Dit beginsel houdt in dat vervolging alleen plaatsvindt indien dit in het algemeen belang is. Bij deze belangenafweging spelen onder meer de ernst van het feit, de omstandigheden van het geval en het vervolgingsbeleid van het OM een rol.

In uitzonderlijke situaties zou het OM ervoor kunnen kiezen om een terughack niet te vervolgen, bijvoorbeeld wanneer het handelen zorgvuldig is verlopen, de schade beperkt is gebleven en er geen maatschappelijk belang is bij strafvervolging. Dit betreft echter een discretionaire bevoegdheid van het OM, die per individueel geval wordt beoordeeld. Tegen een sepotbeslissing staat bovendien op grond van **artikel 12 Sv** beklag open bij het gerechtshof. Hoewel deze route in theorie ruimte laat voor maatwerk, biedt zij geen structurele of voorspelbare oplossing voor de vraag of terughacken toelaatbaar is onder het strafrecht.

Inzet van politievrijwilligers

Een laatste optie die in gesprekken met experts is langsgekomen, is het inzetten van PIR-partijen als politievrijwilligers. Ook dit is geen optie, omdat het een belangenverstrengeling met zich brengt. Ethische hackers die werkzaam zijn bij een PIR-partij moeten in hun functie de belangen van het slachtoffer, hun klant, vooropzetten. Klanten willen doorgaans dat er zo snel mogelijk schadebeperkend gehandeld wordt. Daar tegenover staat dat als er bij de politie een lopend onderzoek is naar de hackers, het juist in het voordeel van het onderzoek kan zijn om nog af te wachten en verder bewijs tegen de achterliggende criminele organisatie te verzamelen. Deze twee rollen zijn dus niet met elkaar verenigbaar.

Ingrijpen Private Partijen: Wenselijk?

Een effectieve aanpak van cybercriminaliteit vergt meer dan het ingrijpen van opsporingsinstanties. Doordat private partijen slachtoffers van cyberaanvallen bijstaan, hebben zij een unieke positie en kennis die hen in sommige gevallen beter in staat stelt dan de opsporingsinstanties om schade van ransomware-aanvallen te beperken. Dit hoofdstuk onderzoekt in hoeverre de behoefte aan bijstand van private partijen de voorkeur verdient boven het optreden van opsporingsinstanties. Vervolgens onderzoekt het hoofdstuk de fundamentele, rechtsstatelijke bezwaren tegen het privatiseren van terughackbevoegdheden. Daarna verkent het de mogelijkheden om onder deze omstandigheden het terughacken door private partijen werkbaar te maken. Hoewel dit onderzoek over terughacken gaat, gebeurt terughacken in de bredere relaties die een slachtoffer heeft met de politie en met private partijen.

Bijdrage en meerwaarde van privaat handelen

Snel handelen staat centraal bij het beperken van de schade die ontstaat door een ransomware-aanval. Private partijen die slachtoffers van een cyberaanval bijstaan hebben hier een centrale rol in, die de rol van de politie aanvult. Voor partijen die reeds slachtoffer zijn van een aanval, kunnen PIR-partijen een belangrijke rol aannemen: back-ups herstellen, onderzoeken over welke informatie de aanvaller beschikt en of het slachtoffer daar nog over beschikt, de sterkte van de onderhandelingspositie van het slachtoffer jegens de aanvaller evalueren en onderhandelen namens het slachtoffer.

Naast bestaande slachtoffers kunnen private partijen ook betekenisvol zijn voor toekomstige slachtoffers. Want wanneer private partijen voor een bestaand slachtoffer te werk gaan, stuiten zij soms op toegang tot de criminele server waar de aanvaller gegevens van een gehackte partij bewaart. In sommige gevallen staan er back-ups van andere partijen die nog niet gehackt zijn, maar waarvan de aanvaller op korte termijn een aanval wil plegen. Pas wanneer een private partij hier iets mee doet, kan het de schade voor toekomstige slachtoffers voorkomen. Hoewel dit een relatief kleine stap is, gaat deze gepaard met een grote verantwoordelijkheid en juridische onzekerheid, zoals besproken in het vorige hoofdstuk. Naast het feit dat private partijen een centrale rol spelen in het bijstaan van een slachtoffer tijdens een ransomware-aanval, gaat de voorkeur van het slachtoffer om verschillende redenen uit naar private bijstand in plaats van ingrijpen door de politie.

Ten opzichte van de betrokkenheid van de politie hebben private partijen dus een complementaire rol voor het slachtoffer. De politie richt "zich in haar brede bestrijdingsstrategie op opsporing, preventie en verstoring" van cybercriminaliteit.[15] De rol van de private partij wordt gekenmerkt door het bijstaan van één specifiek slachtoffer.

Maar de politie zal niet altijd betrokken worden, want slachtoffers van cybercrime doen om verschillende redenen niet altijd aangifte:

- Ten eerste vereist het doen van aangifte dat het slachtoffer gevoelige gegevens deelt of toegang verleent tot digitale systemen. Dit vormt voor veel slachtoffers een drempel, mede vanwege zorgen over privacy en controle over de verstrekte informatie;
- Ten tweede biedt aangifte doen geen garantie dat de zaak daadwerkelijk wordt opgepakt. Cybercrimezaken krijgen relatief weinig prioriteit en middelen, mede omdat opsporing als technisch complex en arbeidsintensief wordt beschouwd.[16] Dit leidt vaak tot frustratie bij slachtoffers;
- Ten derde kan de afweging om een zaak op te pakken in strijd zijn met bredere beleidsprioriteiten. Wanneer de kans op succesvolle opsporing gering wordt geacht, kan ervoor worden gekozen de zaak niet in behandeling te nemen.
- Tot slot kampt de politie met structurele capaciteitsproblemen op het gebied van cyberveiligheid, waaronder een tekort aan gespecialiseerde kennis, technische expertise en gekwalificeerd personeel.[17]

Zelfs wanneer een aangifte wordt opgepakt, lopen de prioriteiten van de politie en de belangen van het slachtoffer niet noodzakelijkerwijs parallel. De politie richt zich by cybercrime primair op het vergaren van bewijs ten behoeve van het vervolgingsdossier, en niet op schadebeperking of directe ondersteuning van het slachtoffer.[18] Juist een PIR-partij vervult hierin een aanvullende rol: zij biedt ondersteuning aan het slachtoffer en kan, indien nodig, het contact met de politie verzorgen. In sommige gevallen is onmiddellijk handelen vereist, bijvoorbeeld om de verspreiding van malware tegen te gaan of andere bedrijven tijdig te waarschuwen. Binnen de respons op een ransomware-aanval is daarom een belangrijke rol weggelegd voor private partijen, die het slachtoffer vaak sneller en effectiever kunnen bijstaan dan de politie.

Tussenconclusie

De inzet van private partijen binnen de cyberverdediging is in deze context minder het resultaat van een bewuste taakverdeling, dan een pragmatische noodzaak: een responsstructuur die voortkomt uit beperkingen in capaciteit en mandaat bij publieke instanties.

Rechtsstatelijke bezwaren

Op staten rust een positieve verplichting om de veiligheid van burgers actief te waarborgen, zo blijkt uit verschillende internationale mensenrechtenverdragen, zoals het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Dit houdt in dat de overheid effectieve maatregelen moet nemen tegen (digitale) dreigingen, ook indien deze afkomstig zijn van derden, zoals bij cyberaanvallen. Tegelijkertijd heeft de staat ook een negatieve verplichting: zij dient zich te onthouden van inmenging in fundamentele rechten.

In de context van hack-backs is artikel 8 EVRM van bijzonder belang. Dit artikel beschermt het recht op respect voor iemands privéleven, familie- en gezinsleven, woning en correspondentie (lid 1), en zo ook de integriteit van iemands computer. Een beperking van dit grondrecht is slechts gerechtvaardigd indien zij berust op een wettelijke grondslag, een legitiem doel dient en voldoet aan de eisen van noodzakelijkheid en proportionaliteit in een democratische samenleving (lid 2).

Om positieve verplichtingen uit te voeren beschikt de staat over bijzondere bevoegdheden, zoals opsporings- en handhavingsmiddelen (inclusief digitale instrumenten), die onder omstandigheden verregaand kunnen ingrijpen in de rechten van burgers. Deze bevoegdheden zijn onderdeel van het geweldsmonopolie. Om te voorkomen dat deze middelen grondrechten schenden, kunnen zij alleen worden ingezet met strikte rechtsstatelijke waarborgen, waaronder het legaliteitsbeginsel, rechterlijke toetsing en democratische verantwoording.

Private partijen beschikken daarentegen niet over een vergelijkbaar juridisch kader. Zij zijn niet democratisch gelegitimeerd, vallen niet onder onafhankelijk toezicht, en zijn niet gehouden tot het naleven van grondrechtelijke proportionaliteitstoetsen of openbaarheidsplichten. Wanneer zij overgaan tot zogenaamde ‘hack backs’, maken zij in wezen gebruik van middelen die raken aan het geweldsmonopolie van de staat, zonder gebonden te zijn aan de rechtsstatelijke waarborgen die daaraan

normaliter verbonden zijn. Dit brengt wezenlijke risico's met zich voor de rechtszekerheid, de rechtsgelijkheid en de bescherming van fundamentele rechten.

Zolang terug-hackhandelingen van PIR-partijen niet onder publiekrechtelijk toezicht staan, bestaan er dan ook serieuze risico's op disproportioneel optreden, willekeur en gebrek aan transparantie.[19] Zonder wettelijke kaders ontbreekt toetsing op noodzakelijkheid en proportionaliteit, waardoor ingezette middelen mogelijk niet in verhouding staan tot het doel. Toegang verkrijgen tot een exfiltratieserver of gehackte gegevens kan bijvoorbeeld een ernstige inbreuk vormen op het recht op privéleven, zoals beschermd onder artikel 8 EVRM.

Daarnaast is sprake van risico op willekeur en eigenrichting, omdat PIR-partijen geen uniforme gedragsnormen of ethische richtlijnen hanteren. Uit interviews blijkt dat de risico-inschatting en morele afwegingen per partij sterk verschillen, wat kan leiden tot ongelijke en onvoorspelbare interventies, ook ten aanzien van onterecht geïdentificeerde doelwitten. Ook is er een structureel gebrek aan transparantie. In tegenstelling tot overheidsinstanties zijn PIR-partijen niet wettelijk verplicht om hun handelen publiekelijk toe te lichten. Transparantie is echter cruciaal om fouten, disproportionele maatregelen of misbruik onafhankelijk te kunnen beoordelen. Tegelijkertijd maken de aard van de werkzaamheden en de gevoeligheid van de betrokken informatie volledige openbaarheid lastig. Het openbaar maken van operationele werkwijzen kan cybercriminelen juist helpen, terwijl het delen van concrete praktijkvoorbeelden vaak gepaard gaat met privacygevoelige informatie. Verder waarschuwen academische bronnen dat de eigenrichting door PIR-partijen ook een escalatie kan uitlokken tussen cyberaanvallers en slachtoffers.[20]

Beperkte Bevoegdheden

Hoewel het privatiseren van hack-backs aanzienlijke rechtsstatelijke risico's met zich meebrengt, valt niet te negeren dat PIR-partijen in de praktijk vaak als enige over de benodigde technische expertise, snelheid en toegang beschikken om directe schade te beperken. In acute situaties, zoals bij toegang tot een exfiltratieserver, zijn zij soms de enige actoren die effectief kunnen handelen om verdere slachtoffers te voorkomen. Daardoor rijst de vraag onder welke voorwaarden terughacken door PIR-partijen toelaatbaar is en slechts een miniem rechtsstatelijk risico vormt.

Voorgestelde voorwaarden voor terughacken

Gelet op het bovenstaande zullen strikte voorwaarden moeten worden verbonden aan het terughacken door PIR-partijen, wil dit passen binnen rechtsstatelijke kaders. Hierbij kan worden gedacht aan:

1. Vergunningenstelsel met beperkte reikwijdte: slechts een beperkt aantal private bedrijven met aantoonbare technische expertise en integriteit komt in aanmerking voor een vergunning.[21] Deze partijen mogen slechts opereren onder toezicht van een daartoe aangewezen bestuursorgaan en altijd in samenwerking met de politie. Zij handelen uitsluitend namens getroffen slachtoffers en binnen het vooraf goedgekeurde mandaat.
2. Duidelijke juridische kaders: de inzet van terughackbevoegdheden dient te voldoen aan het legaliteitsbeginsel en aan de eisen van proportionaliteit en subsidiariteit.[22] Er moeten heldere, in regelgeving vastgelegde grenzen worden gesteld aan toegestane handelingen, toegangsbevoegdheden en gegevensverwerking.
3. Minimale impact, maximale verantwoording: terughackacties moeten tijdelijk en technisch herleidbaar zijn. Elke handeling dient volledig te worden gelogd en achteraf te worden verantwoord aan een onafhankelijke publieke toezichthouder, om toetsing en controle op rechtmatigheid te garanderen.[23]

Tussenconclusie

Vanuit een rechtsstatelijk perspectief vormt het privatiseren van hack-backs een fundamenteel probleem. Het brengt aanzienlijke risico's met zich mee op willekeurig optreden, ongelijke rechtsbescherming en potentieel schadelijk handelen zonder adequate verantwoording. Tegelijkertijd is het een feit dat private partijen in de praktijk vaak sneller en technisch effectiever kunnen optreden dan de politie. De oplossing voor dit spanningsveld ligt dan ook niet in een absolute keuze tussen verbieden of toestaan, maar in het zeer beperkt en zorgvuldig gereguleerd toekennen van hack-backbevoegdheden aan private partijen. In het volgende hoofdstuk wordt besproken onder welke voorwaarden een dergelijk model juridisch verdedigbaar zou kunnen zijn.

Vergunningenstelsel voor ethisch hacken

Zoals in de voorgaande hoofdstukken uiteengezet, zijn hack-backs door private partijen op dit moment strafbaar onder artikel 138ab Sr. Ook een beroep op strafuitsluitingsgronden biedt in de praktijk weinig soelaas. Indien men hack-backs door PIR-partijen toch mogelijk wil maken, zal dit vergunningstechnisch in een wettelijk kader verankerd moeten worden. Met andere woorden: een expliciete uitzonderingsgrond of bevoegdheid moet in het recht worden ingevoerd om dergelijke handelingen toe te staan.

Dit zal waarschijnlijk via het bestuursrecht moeten gebeuren, bijvoorbeeld door een vergunningensysteem op te tuigen dat onder strikte voorwaarden bepaalde hack-backhandelingen legaliseert. Een dergelijke vergunning zou ervoor zorgen dat de hack-handeling niet langer als "wederrechtelijk" wordt aangemerkt. In het strafrecht geldt immers het adagium dat een handeling verricht krachtens een wettelijk voorschrift of bevoegd gegeven ambtelijk bevel niet strafbaar is (vgl. art. 42 Sr). Een vergunningstelsel zou aldus een juridische uitzonderingsgrond kunnen creëren, zodat geautoriseerde private cyberacties buiten de strafbaarheid van art. 138ab Sr vallen.

Bij het ontwerpen van een vergunningenmodel voor hack-backs biedt bestaande Nederlandse wet- en regelgeving waardevolle aanknopingspunten. Twee relevante kaders zijn de Wet Computercriminaliteit III (CCIII) en de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr).

Wet Computercriminaliteit III (CCIII)

Met de **CCIII** heeft de wetgever de bevoegdheden van opsporingsdiensten uitgebreid, waaronder het toekennen van een hackbevoegdheid aan politie en justitie onder strikte voorwaarden. Sinds 2019 mag de politie op grond van deze wet heimelijk en op afstand (online) binnendringen in computers van verdachten: de zogenoemde *hackbevoegdheid*. Deze bevoegdheid is opgenomen in het Wetboek van Strafvordering (bijv. art. 126nba Sv) en mag uitsluitend worden ingezet bij ernstige delicten, met machtiging van de rechter-commissaris, en onder toezicht van de Inspectie Justitie en Veiligheid. Het CCIII-kader toont aan dat hacken **mogelijk is binnen de rechtsstaat**, mits er vooraf duidelijk wettelijk mandaat, rechterlijke toetsing en toezicht is. Dit biedt een aanknopingspunt: analoog hieraan zou een vergunning voor private hack-backs eveneens aan strenge voorwaarden en toezicht moeten worden onderworpen.

Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr)

De **Wpbr** reguleert private beveiligingsbedrijven en recherchebureaus via een vergunningenstelsel. Artikel 2, eerste lid Wpbr bepaalt dat *"Het is verboden zonder vergunning van Onze Minister door de instandhouding van een beveiligingsorganisatie of recherchebureau beveiligingswerkzaamheden of recherchewerkzaamheden te verrichten of aan te bieden."* Met andere woorden: particuliere beveiligingsdiensten en detective-activiteiten zijn vergunningsplichtig. Bedrijven moeten bij de screeningsautoriteit Justis een vergunning aanvragen en voldoen aan diverse vereisten.[24] Zo wordt personeel op betrouwbaarheid getoetst, gelden voorschriften voor opleiding, gedrag en geheimhouding, en is er toezicht vanuit de politie op hun werkzaamheden.

Hoewel de Wpbr primair ziet op fysieke beveiliging en traditionele recherche, biedt het conceptuele **aanknopingspunten** voor een cybervergunningstelsel. Net zoals privébewakers beperkt bevoegd zijn en onder toezicht staan, zou men zich een regime kunnen voorstellen waarin private incidentresponsepartijen een speciale vergunning nodig hebben om actieve cyberverdedigingshandelingen te verrichten. De analogie is dat de overheid erkent dat bepaalde veiligheidsactiviteiten door private partijen mogen worden uitgevoerd, maar alleen onder strikte regulering en met overheidscontrole.

Belangrijk is wel dat de huidige Wpbr géén vrijbrief geeft om strafbare middelen te gebruiken. Een private beveiligingsorganisatie mag bijvoorbeeld geen geweld toepassen of opsporingsbevoegdheden uitoefenen die exclusief aan de overheid zijn voorbehouden. Evenzo mogen private recherchebureaus niet inbreken op systemen of telefoons hacken; zij moeten zich houden aan de wet (bijvoorbeeld informatie vergaren via openbare bronnen of met toestemming van betrokkenen). Een Wpbr-vergunning legitimeert dus geen strafbare handelingen, zoals computervredebreuk. Toch laat de Wpbr wel zien dat een vergunningstelsel kan werken om private veiligheidsdiensten binnen kaders toe te laten. Dit principe kan als voorbeeld dienen voor een cybervergunningsmodel, waarin incidentresponsepartijen onder strikte voorwaarden en toezicht bevoegd zijn tot het verrichten van actieve digitale handelingen ter bevordering van cybersecurity.

Samengevat bieden bestaande wetten dus aanknopingspunten: de CCIII toont dat hacken onder strikte voorwaarden wettelijk geregeld kan worden (zij het voor de overheid), terwijl de Wpbr laat zien hoe private veiligheidsactiviteiten onder toezicht en met duidelijke regels kunnen worden toegestaan. In dit verband suggereert ook Couzigou dat, naar het voorbeeld van private maritieme beveiligingsbedrijven

(PMSCs), een beperkt aantal private actoren een licentie zou kunnen krijgen voor actieve cyberverdediging, onder nauw toezicht van de staat. Zo'n model combineert private uitvoeringscapaciteit met publiek toezicht, zonder het juridische monopolie van de staat aan te tasten.[25]

Complicerende factoren bij regulering van hack-backs

Hoewel een vergunningensysteem voor ethisch hacken (hack-backs) juridisch vormgegeven kan worden naar analogie met bestaande kaders zoals de *Wpbr* en de *WCCIII*, doen zich bij het ontwerp verschillende complicerende factoren voor die extra aandacht vereisen.

Internationale verplichtingen

Een belangrijk aandachtspunt bij het vormgeven van een vergunningsstelsel is de verenigbaarheid met internationale verplichtingen. Nederland is partij bij het *Cybercrime Verdrag*, dat staten verplicht om ongeautoriseerde toegang tot computersystemen strafbaar te stellen. De kernbepaling vereist strafbaarstelling van toegang "zonder recht". Hoewel deze formulering op zichzelf ruimte laat voor nationale uitzonderingen, bijvoorbeeld in de vorm van een wettelijke vergunning, heeft geen enkele verdragsstaat deze ruimte benut om hack-backs door private partijen toe te staan.[26] De heersende praktijk binnen het verdrag is dan ook dat dergelijke handelingen strafbaar blijven, ongeacht motief of context.

Daarnaast is Nederland, zoals hierboven is opgemerkt, gebonden aan de *Paris Call for Trust and Security in Cyberspace*, waarin expliciet wordt opgeroepen tot het voorkomen van hack-backs door niet-statelijke actoren. Door deze verklaring te ondertekenen, heeft Nederland zich politiek uitgesproken vóór overheidsregie en tegen digitale vergelding door private partijen. Hoewel de *Paris Call* geen juridisch bindende status heeft, weerspiegelt zij wel een breed gedeelde internationale norm waaraan Nederland zich politiek heeft verbonden.[27] Een vergunningsmodel zou daarom niet alleen juridisch zorgvuldig moeten worden vormgegeven, maar ook afgestemd moeten zijn op deze politieke en diplomatieke context.

Soevereiniteitsvragen en internationaal recht

Naast verdragsverplichtingen zoals het *Cybercrime Verdrag* en de *Paris Call*, brengt ook het bredere internationale rechtskader aanzienlijke complicaties met zich voor een nationaal vergunningensysteem voor hack-backs. Een van de grootste juridische obstakels bij het reguleren van hack-backs is het risico op schending van de soevereiniteit van andere staten. Soevereiniteit houdt in dat staten exclusieve zeggenschap hebben over wat er binnen hun eigen grondgebied gebeurt, inclusief de controle over fysieke

en digitale infrastructuur zoals servers, netwerken en datacenters. Dit geldt niet alleen voor land, binnenwateren en luchtruim, maar ook voor gebieden onder exclusieve controle, zoals oorlogsschepen of bezette gebieden.[28]

De VN-Groep van Regeringsexperts (UNGGE) heeft in haar *rapporten van 2013 en 2015* bevestigd dat dit beginsel onverkort van toepassing is in cyberspace. Staten hebben niet alleen het recht, maar ook de plicht om toezicht te houden op ICT-activiteiten binnen hun grenzen, of die nu worden uitgevoerd door publieke of private actoren, en of de herkomst nu binnenlands of buitenlands is.[29] Daar wringt het bij hack-backs. Zulke digitale tegenmaatregelen hebben vrijwel altijd een grensoverschrijdend karakter: ze richten zich op netwerken buiten het domein van het slachtoffer, en dringen daarbij vaak binnen in infrastructuur op het grondgebied van een andere staat. Daarmee is het risico groot dat de soevereiniteit van die staat wordt geschonden.

Volgens de *Tallinn Manual 2.0* (een gezaghebbende maar niet-bindende handleiding opgesteld door een groep internationale experts onder leiding van het NATO Cooperative Cyber Defence Centre) is van zo'n schending sprake zodra een cyberoperatie significante fysieke schade veroorzaakt of de functionaliteit van systemen in een andere staat aantast. Zelfs als er geen zichtbare schade is, maar onderdelen gerepareerd of vervangen moeten worden, wordt dit in veel gevallen al als een schending beschouwd. Hoewel er geen volledige internationale consensus is over de precieze grens, is de onderliggende lijn duidelijk: ongeautoriseerde cyberacties die ingrijpen in buitenlandse infrastructuur zijn juridisch problematisch.[30]

Als de gevolgen van een hack-back ernstig genoeg zijn, kan zo'n actie zelfs worden aangemerkt als verboden geweld onder *artikel 2(4) van het VN-Handvest*. In dat geval mag het niet eens als tegenmaatregel worden uitgevoerd, en kan ook een nationale vergunning geen rechtsgrond bieden, omdat het geweldsverbod internationaal dwingend recht is.[31]

Kortom: wie hack-backs door private partijen wil reguleren, moet niet alleen kijken naar nationale wetgeving, maar ook naar de implicaties voor het internationaal recht. Zolang het risico op soevereiniteitsschending of schending van het geweldsverbod blijft bestaan, blijft deze route juridisch en diplomatiek uiterst precair.

Internationale terughoudendheid en ontbreken van consensus

De juridische en diplomatieke gevoeligheid van hack-backs wordt versterkt door het feit dat er wereldwijd geen internationale consensus bestaat over de toelaatbaarheid ervan, laat staan over regulering via een nationaal vergunningensysteem. In de praktijk blijkt dat staten terughoudend blijven en nadrukkelijk kiezen voor centrale overheidsregie bij cyberverdediging, waarbij zij private vergeldingsacties afwijzen.

Een sprekend voorbeeld van de internationale verdeeldheid is het *Amerikaanse ACDC-wetsvoorstel (Active Cyber Defense Certainty Act)*. Met dit voorstel, dat tussen 2017 en 2019 herhaaldelijk werd ingediend in het Amerikaanse Congres, werd beoogd om private partijen onder strikte voorwaarden toe te staan om hack-backs uit te voeren. Alleen slachtoffers van een "aanhoudende ongeautoriseerde inbraak" zouden, na voorafgaande kennisgeving aan de FBI, gerechtigd zijn om beperkte digitale tegenmaatregelen te treffen. De toegestane doelen waren onder andere het achterhalen van de identiteit van de aanvaller, het beëindigen van lopende aanvallen en het verzamelen van inlichtingen ter versterking van de eigen verdediging.[32]

Hoewel het wetsvoorstel strikte waarborgen bevatte, waaronder een verbod op het veroorzaken van fysieke schade, economische schade of risico's voor de openbare veiligheid, is het voorstel uiteindelijk nooit aangenomen. De voornaamste bezwaren betroffen het risico op escalatie van cyberconflicten, de inherente onzekerheid van attributie in cyberspace, de kans op nevenschade aan derden (bijvoorbeeld via gecompromitteerde tussencomputers) en de ondermijning van het staatsmonopolie op legitiem geweld**.** Daarnaast werd gewezen op de mogelijke strijdigheid met het internationaal recht en het risico dat dergelijke acties buitenlandse wetgeving zouden schenden en diplomatieke spanningen zouden veroorzaken.[33]

Hoewel initiatieven zoals het *ACDC-wetsvoorstel* in de Verenigde Staten pleiten voor gereguleerde hack-backs door private partijen, wijst de internationale praktijk in een andere richting. De overwegende internationale consensus is dat de risico's, zoals escalatie, foutieve attributie en inbreuk op buitenlandse wetgeving, zwaarder wegen dan de potentiële voordelen. Zolang er geen breed gedragen internationaal verdrag bestaat dat hack-backs onder strikte voorwaarden toestaat, is het weinig aannemelijk dat individuele landen deze praktijk zelfstandig zullen legaliseren zonder aanzienlijke geopolitieke risico's te lopen.

Complexe afbakening en reguleringslast

Een probleem bij een vergunningensysteem voor hack-backs is de praktische uitvoerbaarheid, vanwege de noodzakelijke precieze afbakening van begrippen zoals 'proportionaliteit', 'noodzaak' en een 'hoge mate van zekerheid' bij attributie.

Proportionaliteit en noodzaak

Proportionaliteit houdt in dat een hack-back in verhouding moet staan tot de aanval waarop wordt gereageerd, waarbij maatregelen gericht, tijdelijk en bij voorkeur omkeerbaar dienen te zijn. Vergeldingsacties of het aanrichten van bredere digitale schade vallen daar niet onder. In de praktijk is dat vaak moeilijk te waarborgen.[34] De impact van een hack-back is zelden volledig voorspelbaar. Het risico op nevenschade is groot.

Het noodzakelijkheidsvereiste houdt in dat een hack-back alleen is toegestaan wanneer minder ingrijpende alternatieven, zoals netwerkisolatie, het verhelpen van kwetsbaarheden of het inzetten van honeypots, aantoonbaar niet volstaan.[35] Voor PIR-partijen, die vaak onder hoge tijdsdruk opereren en slechts beperkt zicht hebben op het volledige dreigingsbeeld, is het buitengewoon lastig om dit zorgvuldig en tijdig te beoordelen, laat staan overtuigend te documenteren. Dit leidt niet alleen tot juridische onzekerheid, maar ook tot een aanzienlijke verantwoordingsdruk voor zowel de aanvragers als de toezichthoudende instantie.[36]

Het risico op aansprakelijkheid of het verlies van een vergunning kan bovendien leiden tot een zogenoemd *chilling effect*, waarbij verdedigend optreden juist wordt afgeremd op momenten van acute dreiging.[37]

Hoge mate van zekerheid bij attributie

Een groot probleem bij actieve cyberdefensie is de onzekerheid rond attributie (het vaststellen wie achter een aanval zit). Aanvallers gebruiken veelvuldig technieken om hun identiteit te verbergen.[38]Hierdoor is het zelden mogelijk om met voldoende zekerheid vast te stellen wie daadwerkelijk verantwoordelijk is voor een aanval. Het risico op misattributie is reëel, met mogelijk ernstige nevenschade voor onschuldige actoren.

Uitvoerbaarheid van toezicht en vergunningverlening

Een vergunningensysteem vergt voor deze complexe afwegingen voortdurende beoordeling door juridisch én technisch onderlegde toezichthouders. Dit brengt een aanzienlijke toezichtsinspanning met zich, en vraagt om voldoende flexibiliteit om in te kunnen spelen op technologische ontwikkelingen en wisselende dreigingen. Daarnaast brengt een dergelijk stelsel administratieve lasten met zich mee voor zowel de PIR-partijen als de toezichthouders, wat procedurele vertraging veroorzaakt in reactie op cyberdreigingen.

Nevenschade en aansprakelijkheid

Hack-backs brengen een reëel risico op nevenschade met zich mee. Cyberaanvallen worden vaak gerouteerd via servers van onschuldige derde partijen.[39] Als een private partij op basis van foutieve attributie een server aanvalt die slechts als tussenstation werd gebruikt, kunnen onschuldige slachtoffers getroffen worden.[40] Bovendien kunnen hack-back-operaties schade veroorzaken aan vitale infrastructuur of persoonsgegevens van derden, wat juridische aansprakelijkheid met zich meebrengt.[41] Zelfs indien een vergunningensysteem wordt ingevoerd, zou aansprakelijkheid voor dergelijke schade vermoedelijk blijven rusten op de uitvoerende partij (of staat).[42] De vraag in hoeverre PIR-partijen aansprakelijk kunnen worden gesteld voor schade als gevolg van hack-back-operaties valt buiten de reikwijdte van dit onderzoek, maar verdient nadere beschouwing in toekomstig onderzoek.

Relevantie van Wpbr voor hack-backhandelingen door PIR-partijen

De Wpbr biedt een vergunningenkader dat uitgaat van:[43]

- Definities voor de twee soorten handelingen die de wet reguleert, namelijk ‘beveiligingswerkzaamheden’ en ‘recherchewerkzaamheden’ (art. 1);
- Een vergunningsplicht voor dergelijke handelingen (art. 2) en middelen om deze vergunning in te trekken wanneer niet aan de criteria wordt voldaan (artt. 14-17);
- Categorisering van actoren die in aanmerking komen voor een vergunning (art. 3);
- Criteria bij het verlenen van een vergunning, zoals betrouwbaarheid en een zorgvuldigheidsnorm (artt. 4-4a);
- Verplichtingen en kwaliteitsstandaarden waaraan moet worden voldaan tijdens de beveiligings- of recherchehandelingen (artt. 5-10). Denk daarbij aan verslaglegging, een klachtenstelsel, medische geschiktheid, opleidingseisen en uniform en apparatuur;
- Bevoegdheden voor toezicht en handhaving (art. 11 e.v.).

Tussenconclusie

De systematiek van de Wpbr past in beginsel binnen het Nederlandse bestuursrecht en biedt waardevolle aanknopingspunten voor het opzetten van een vergunningensysteem voor ethisch hacken. Een dergelijke vertaalslag vereist wel verdere juridische en technische uitwerking, maar lijkt op hoofdlijnen verenigbaar met de uitgangspunten van legaliteit, toezicht en bescherming van grondrechten.

Conclusie

De bestrijding van ransomware-aanvallen in Nederland staat onder druk. Waar publieke instanties als de politie en het OM traditioneel gezien verantwoordelijk zijn voor opsporing en vervolging, blijkt in de praktijk dat private incident response-partijen (PIR's) onmisbaar zijn in het beperken en voorkomen van schade. Deze ontwikkeling is deels ingegeven door structureel capaciteitsgebrek bij de overheid en deels door de technologische voorsprong en het reactievermogen van private actoren. PIR's bevinden zich hierdoor steeds vaker in een juridische onzekere en ongelegitimeerde zone, met name wanneer zij, uit oogpunt van schadebeperking, overwegen terug te hacken of data veilig te stellen van exfiltratieservers.

Uit dit onderzoek blijkt echter dat het huidige juridische kader nauwelijks ruimte laat voor zulke handelingen. Artikel 138ab Sr stelt computervredebreuk strafbaar zonder uitzondering voor ethisch hacken. Beroep op bestaande strafuitsluitingsgronden biedt slechts in uitzonderlijke gevallen een uitweg. Ook het opportuniteitsbeginsel van het OM biedt onvoldoende aanknopingspunten. Bovendien echoën internationale verdragen en toezeggingen zoals het Cybercrimeverdrag en de Paris Call de reeds bestaande gedachte dat hack-backs door private partijen in beginsel moeten worden voorkomen.

Tegelijkertijd is duidelijk geworden dat het weren van PIR's uit deze responsfase niet realistisch is: zij beschikken vaak als enige over de noodzakelijke toegang, technische middelen en snelheid om verdere schade of slachtoffers te voorkomen. Deze spanning tussen juridische onmogelijkheid en feitelijke noodzaak vormt de kern van het probleem.

Een vergunningensysteem zou op termijn juridische ruimte kunnen creëren, mits het voldoet aan strikte voorwaarden van proportionaliteit, toezicht en transparantie. Bestaande kaders zoals de Wpbr en de Wet Computercriminaliteit III bieden daarbij nuttige aanknopingspunten. Toch kleven er substantiële juridische en praktische bezwaren aan een dergelijk systeem. Internationale rechtsregels stellen grenzen aan digitale acties over landsgrenzen heen. Het risico op nevenschade en escalatie is reëel, en het toezicht op en de uitvoeringscapaciteit van PIR's is nu nog onvoldoende geborgd.

Het paper laat dan ook zien dat een onmiddellijke legalisering van private hack-backs onverantwoord is. De huidige wet biedt daar geen ruimte voor, en een beleidsmatige opening zonder heldere waarborgen

zou rechtsstatelijke principes ondermijnen. Tegelijkertijd is het evenmin houdbaar om de bijdrage van PIR's volledig te negeren. De oplossing ligt in een voorzichtige, graduele benadering: versterk de publieke capaciteit, ontwikkel heldere samenwerkingskaders tussen publieke en private partijen, en onderzoek in internationaal verband onder welke voorwaarden gereguleerd terughacken in de toekomst toelaatbaar zou kunnen zijn. Alleen zo kan Nederland toewerken naar een robuuste en rechtsstatelijk verantwoorde cyberverdediging.

---

[1] HR 28 januari 2011, ECLI:NL:HR:2011:BN9287, r.o. 2.4.
[2] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 32.
[3] Openbaar ministerie, *Leidraad Responsible Disclosure* 2018 ro. 4.2.
[4] Rb. Oost-Brabant 13 februari 2013, ECLI:NL:RBOBR:2013:BZ1157.
[5] Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (LL.M.-scriptie Law and Technology, Tilburg University), Tilburg: TILT 2021.
[6] Paris Call for Trust and Security in Cyberspace, *The 9 Principles*, geraadpleegd 18 juni 2025, (https://pariscall.international/en/principles).
[7] *Kamerstukken II*, 2016/17, 34372, nr. 6, p. 66 (https://zoek.officielebekendmakingen.nl/kst-34372-6.html#:~:text=een geautomatiseerd werk echter niet,De eigenaar van een).
[8] Openbaar Ministerie, *Richtlijn voor strafvordering cybercrime*, Stcrt. 2020, 22034.
[9] W. van der Wagen, E.G. van 't ZandKurtovic-, S.R. Matthijsse, T.F.C. Fischer, *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin. Eindrapportage*, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) / Ministerie van Justitie en Veiligheid, Den Haag december 2019.
[10] P.A.M. Mevis, Capita Strafrecht, Ars Aequi Libri, Nijmegen 2013, p. 820.
[11] P.A.M. Mevis, Capita Strafrecht, Ars Aequi Libri, Nijmegen 2013, p. 823.
[12] HR 22 maart 2016, ECLI:NL:HR:2016:456.
[13] Zie: Noyon/Langemeijer/Remmelink, aant. 4 op art. 41 (bijgewerkt tot 6 december 2022).
[14] HR 20 februari 1933, ECLI:NL:HR:1933:229 (*Veearts*).
[15] Politie 2024, *Begroting en beheerplan 2025-2029*, p. 9.
[16] Borwell, Jansen, Stoll 2024, Recht doen aan de behoeften van cybercrimeslachtoffers: reflecties op de rol van de politie, p. 47-48.
[17] Politie 2024, *Begroting en beheerplan 2025-2029*, p. 23.
[18] Politie 2024, *Begroting en beheerplan 2025-2029*, p. 9.
[19] Couzigou, I. (2020). Hacking-Back by Private Companies and the Rule of Law. *Heidelberg Journal of International Law*, *80*(2), p. 500-501.
[20] Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (LL.M.-scriptie Law and Technology, Tilburg University), Tilburg: TILT 2021. I. Couzigou, 'Hacking-Back by Private Companies and the Rule of Law' 2020 Heidelberg Journal of International Law 80, p. 501.
[21] I. Couzigou, 'Hacking-Back by Private Companies and the Rule of Law' 2020 Heidelberg Journal of International Law 80, p. 505.
[22] I. Couzigou, 'Hacking-Back by Private Companies and the Rule of Law' 2020 Heidelberg Journal of International Law 80, p. 506.
[23] I. Couzigou, 'Hacking-Back by Private Companies and the Rule of Law' 2020 Heidelberg Journal of International Law 80, p. 507.

[24] Justis 2024, *Wat is de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr)? (*https://www.justis.nl/producten/particuliere-beveiliging-en-recherche/wat-is-de-wet-particuliere-beveiligingsorganisaties-en-recherchebureaus-wpbr).
[25] Irene Couzigou, *Hacking-Back by Non-State Actors and the Rule of Law*, ECIGL Working Paper (2020), te raadplegen via (https://www.law.ed.ac.uk/sites/default/files/2020-09/ECIGL Working Paper - I Couzigou_0 - Acc.pdf).
[26] Irene Couzigou, *Hacking-Back by Non-State Actors and the Rule of Law*, ECIGL Working Paper 2020, te raadplegen via: https://www.law.ed.ac.uk/sites/default/files/2020-09/ECIGL%20Working%20Paper%20-%20I%20Couzigou_0%20-%20Acc.pdf, p. 492 e.v; en Philippe Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (masterscriptie LL.M. Law and Technology, Tilburg University januari 2021), te raadplegen via https://arno.uvt.nl/show.cgi?fid=155524, p. 33 e.v.
[27] Idem.
[28] Irene Couzigou, *Hacking-Back by Non-State Actors and the Rule of Law*, ECIGL Working Paper (2020), te raadplegen via https://www.law.ed.ac.uk/sites/default/files/2020-09/ECIGL%20Working%20Paper%20-%20I%20Couzigou_0%20-%20Acc.pdf, p. 481 e.v.
[29] Karine Bannelier and Théodore Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale, 2017), te raadplegen via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988, p. 13.
[30] Karine Bannelier and Théodore Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale, 2017), te raadplegen via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988, p. 44.
[31] Karine Bannelier and Théodore Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale, 2017), te raadplegen via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988, p. 48.
[32] Philippe Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (masterscriptie LL.M. Law and Technology, Tilburg University januari 2021), te raadplegen via https://arno.uvt.nl/show.cgi?fid=155524, p. 22 e.v; en Dennis Broeders, 'Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?' (2021) 7 *Journal of Cybersecurity* https://scholarlypublications.universiteitleiden.nl/access/item%3A3249232/view accessed 20 June 2025.
[33] Philippe Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (masterscriptie LL.M. Law and Technology, Tilburg University januari 2021), te raadplegen via https://arno.uvt.nl/show.cgi?fid=155524, p. 22 e.v; en Dennis Broeders, 'Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?' (2021) 7 *Journal of Cybersecurity* https://scholarlypublications.universiteitleiden.nl/access/item%3A3249232/view accessed 20 June 2025.
[34] Irene Couzigou, *Hacking-Back by Non-State Actors and the Rule of Law*, ECIGL Working Paper (2020), teraadplegen via https://www.law.ed.ac.uk/sites/default/files/2020-09/ECIGL%20Working%20Paper%20-%20I%20Couzigou_0%20-%20Acc.pdf, p. 500 e.v.
[35] Philippe Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (masterscriptie LL.M. Law and Technology, Tilburg University, januari 2021), te raadplegen via: https://arno.uvt.nl/show.cgi?fid=155524, hfdst. III *Hacking Back and the ACDC Bill in the United States*, §§ 4.3.2.
[36] Philippe Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (masterscriptie LL.M. Law and Technology, Tilburg University, januari 2021), te raadplegen via: https://arno.uvt.nl/show.cgi?fid=155524, hfdst. IV *Assessing the merits of decriminalizing hacking back in the Netherlands*, § 4.3.2.
[37] Philippe Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (masterscriptie LL.M. Law and Technology, Tilburg University, januari 2021), te raadplegen via: https://arno.uvt.nl/show.cgi?fid=155524, hfdst. III *Hacking Back and the ACDC Bill in the United States*, §§ 3.3.3.
[38] Karine Bannelier and Théodore Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale, 2017), te raadplegen via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988, p. 45.

[39] Cybersecurity Tech Accord, *No Hacking Back: Vigilante Justice vs. Good Security Online – A Policy Maker's Guide to Knowing the Difference*, november 2020, p. 12, te raadplegen via https://cybertechaccord.org/uploads/prod/2020/11/hack-back-update-131120-pages.pdf.
[40] Philippe Martens, *Self-defence in Cyberspace: Hacking Back the Hacker. Exploring the merits of decriminalizing hacking back by non-state actors in the Netherlands* (masterscriptie LL.M. Law and Technology, Tilburg University, januari 2021), te raadplegen via: https://arno.uvt.nl/show.cgi?fid=155524, hfdst. III *Difficulties in Establishing Attribution and Risk of Collateral Damage*, § 3.5.2.
[41] Cybersecurity Tech Accord, *No Hacking Back: Vigilante Justice vs. Good Security Online – A Policy Maker's Guide to Knowing the Difference*, november 2020, p. 11, te raadplegen via https://cybertechaccord.org/uploads/prod/2020/11/hack-back-update-131120-pages.pdf.
[42] Irene Couzigou, *Hacking-Back by Non-State Actors and the Rule of Law*, ECIGL Working Paper (2020), te raadplegen via https://www.law.ed.ac.uk/sites/default/files/2020-09/ECIGL%20Working%20Paper%20-%20I%20Couzigou_0%20-%20Acc.pdf, p. 503-507.
[43] Zie Wet particuliere beveiligingsorganisaties en recherchebureaus, te raadplegen via: https://wetten.overheid.nl/BWBR0042108/2020-04-29; Justis, "Wat is de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr)?", https://www.justis.nl/producten/particuliere-beveiliging-en-recherche/wat-is-de-wet-particuliere-beveiligingsorganisaties-en-recherchebureaus-wpbr.