Allereerst wil ik bij deze uw commissie hartelijk danken voor de uitnodiging om namens Nederland ICT te spreken bij een rondetafelgesprek over het wetsvoorstel computercriminaliteit III. Nederland ICT is een voorstander om computercriminaliteit aan te pakken en begrijpt dan ook de wens van de overheid om nieuwe bevoegdheden te introduceren in de wet Computercriminaliteit III. Echter Nederland ICT vraagt zich wel af of in de nieuwe wet de juiste balans is gezocht tussen collectieve veiligheid en individuele vrijheden, of de wet Nederland niet kwetsbaarder maakt in plaats van veiliger, of niet een onevenredig grote inbreuk op de grondrechten wordt gemaakt en of de wet geen enorme economische schade gaat toebrengen.

Ten opzichte van de concept versie uit 2013(!) is er een aantal verbeteringen aangebracht: de verplichting tot ontsleuteling is er uit, waardoor je niet meer hoeft mee te werken aan je eigen veroordeling. Ook is het positief dat helers van computergegevens strafbaar worden gesteld, waardoor hackers die bijvoorbeeld buitgemaakte persoonsgegevens willen verhandelen strafbaar gesteld kunnen worden. Echter met de Wet Computercriminaliteit III introduceert het kabinet ook een nieuwe bevoegdheid: het heimelijk binnendringen van een geautomatiseerd werk. Dit betekent concreet het mogen hacken van apparatuur zoals computers en mobiele telefoons, maar ook het hacken van clouds en slimme energiemeters valt onder de bevoegdheid. Nederland ICT vindt het onwenselijk wanneer de politie dit middel mag inzetten. Het verhogen van de de strafmaat naar een minimale celstraf van 8 jaar doet daar niets aan af. Ik leg u graag uit waarom.

Nederland heeft nu een zeer sterke positie op het gebied van internet. We waren nauw betrokken bij de totstandkoming van het internet en worden internationaal nog steeds gezien als autoriteit op het gebied van internet governance en voorvechter van een vrij en open internet. Met heldere standpunten op het gebied van netneutraliteit en recent nog encryptie gooit Nederland internationaal gezien hoge ogen. Het vestigingsklimaat is goed en er ontstaan op het moment allerlei veelbelovende startups. We hebben deze sterke positie te danken aan het feit dat de bevolking hoog opgeleid is, praktisch iedereen voorzien is van snelle vaste en mobiele internetverbindingen en Nederland met AMS-IX de beschikking heeft over één van de grootste internetknooppunten ter wereld. Recente investeringen van grote bedrijven als Google, IBM en Microsoft en het flinke aantal techstartups onderschrijven de sterke positie van Nederland en het vertrouwen dat bestaat in de Nederlandse internet en technologiesector. Hierdoor heeft Nederland de potentie om proeftuin voor nieuwe ICT-toepassingen te worden.

Echter vertrouwen in ICT is essentieel om deze positie te behouden: vertrouwen dat niemand meeleest met de communicatie, vertrouwen dat diegene met wie je communiceert ook daadwerkelijk is wie hij of zij zegt. Vertrouwen dat je data vertrouwelijk blijft en niet op straat komt te liggen en tenslotte het vertrouwen dat de diensten en apparaten waar je gebruik van maakt betrouwbaar zijn. Nederland ICT vindt de bevoegdheid om te hacken schadelijk voor dit vertrouwen omdat de wet leidt tot het stimuleren van een industrie van “politie gereedschappen” die er belang bij heeft kwetsbaarheden geheim te houden in plaats van te openbaren. Daarbij komt dat met het gebruik van dergelijke gereedschappen door de complexiteit van ICT-producten en diensten schade aangericht kan worden aan onschuldige omstanders. Dit kan al optreden bij het binnendringen, maar zeker ook bij het plaatsen van “policeware” of het op andere wijzen ingrijpen in geautomatiseerde werken. Ook heeft de hackbevoegdheid een ongewenstneveneffect omdat de politie niet alle kennis in huis heeft. Op deze manier houdt de Nederlandse overheid het bestaan van een zwarte markt van kwetsbaarheden in stand, die het met de wetgeving computercriminaliteit juist wil tegengaan.
Nederland ICT ziet een groeiend spanningsveld tussen een hackbevoegdheid waardoor digitale systemen worden verzwakt, tegenover dezelfde overheid die niet alleen een publiek private samenwerking in het cyberdomein stimuleert, maar ook bedrijven verplicht kwetsbaarheden te

melden in verschillende meldplichten, de Telecomwet of de Europese NIB-richtlijn. Het ene onderdeel van VenJ (NCSC) lijkt zo de strijdt aan te gaan met het andere onderdeel (NP).

De hack bij het Italiaanse Hackingteam vorige zomer, een bedrijf dat handelt in onder meer (zero-day) exploits, liet zien dat de Nederlandse politie alvast kennis kwam ophalen vooruitlopend op computercriminaliteit III. Het antwoord van de overheid na Kamervragen, in augustus 2015, baart Nederland ICT grote zorgen hoe open en transparant de politie zal zijn wanneer zij daadwerkelijk de bevoegdheid tot hacken krijgt. Ik citeer: “dat het verstrekken van informatie over welke specifieke software de opsporingsdiensten beschikken, testen en gebruiken grote risico’s met zich meebrengt voor de inzetbaarheid van die middelen.” Wij vragen dan ook: Kan de overheid garanderen dat ze de gemelde zwakheden niet gebruikt voor offensieve doeleinden? Kan de overheid garanderen dat het Nederlandse bedrijfsleven geen schade gaat ondervinden door de inzet van kwetsbaarheden? Gaat de overheid transparant zijn over het gebruik en de kosten van de hackbevoegdheid? Nog los van de vraag of de Nederlandse overheid überhaupt een dergelijk systeem waarbij bedrijven die handelen in veiligheidlekken zou moeten willen ondersteunen. Een verbod op het gebruik van zogenaamde zero-days exploits zou Nederland ICT dan ook zeer wenselijk vinden.

Ook vindt Nederland ICT het gebruik van technische kwetsbaarheden om binnen te dringen in geautomatiseerde werken door opsporingsinstanties zich niet verstaan met de vrijheden en de bescherming van de persoonlijke levenssfeer van niet-verdachten en omstanders. Het in standhouden en uitnutten van technische kwetsbaarheden is niet in het belang van een veilige en beschermde persoonlijke levenssfeer van burgers. Hoge eisen zullen dan ook gesteld moeten worden aan het specifiek inkaderen van een onderzoek. Met name van data die is opgeslagen in de cloud bestaat het risico dat in een onderzoek uiteindelijk data van veel meer partijen wordt meegenomen. Het zoeken in specifieke datasets zal dan ook zo specifiek mogelijk omschreven moeten worden zijn. Ook moeten we ons realiseren dat voor internationale ICT bedrijven wiens cloud zich onder meer in Nederland bevindt, de wet computercriminaliteit te weinig waarborgen omvat. Want hoe ‘integer’ is hun cloud wanneer de Nederlandse politie mag hacken? Hoe kunnen ze dit hun klanten garanderen? Dit soort onzekerheden waarbij er een disbalans lijkt te ontstaan tussen veiligheid en waarborgen is slecht voor het Nederlandse investeringsklimaat. Ook is Nederland ICT uitermate kritisch op de bevoegdheid om te hacken in het buitenland. In de memorie van toelichting is te lezen dat wanneer het geautomatiseerde werk zich in het buitenland bevindt een rechtshulpverzoek kan worden gedaan, behoudens uitzonderlijke omstandigheden. Vervolgens lezen we dat een verzoek aan een buitenlandse aanbieder tot het vertrekken van informatie over hun klant maar een beperkte kans van slagen heeft bij en ook nog vaak veel tijd kost. Is dit afdoende reden om zo’n zwaar middel in te zetten? Wij vinden van niet. Nederland ICT vindt dat de internationaal rechtelijke processen gevolgd moeten worden (bijstandsverzoeken vreemde overheden). En Nederland ICT is een groot pleitbezorger van samenwerking tussen politie en ICT-bedrijven, ook in internationaal verband.

Nederland ICT vraagt dan ook een grote betrokkenheid vanuit de politiek. De politiek dient kritisch te kijken naar de noodzaak van vergaande verruiming van de bevoegdheden voor de politie. Er is een spanningsveld tussen vrijheid en veiligheid, tussen Veiligheid en Justitie. Willen we in Nederland een publiek-private samenwerking op gang brengen zoals het Nationaal Cyber Security Centrum die voorstaat of willen we een overheid die er gebaat bij is kwetsbaarheden in stand te houden? Willen we een overheid die enerzijds pleit voor internationale samenwerking in het cyberdomein, om vervolgens op eigen houtje in te breken op systemen in het buitenland?. Het is nu aan de Tweede Kamer om te kiezen tussen deze twee gezichten.

Liesbeth Holterman, Nederland ICT