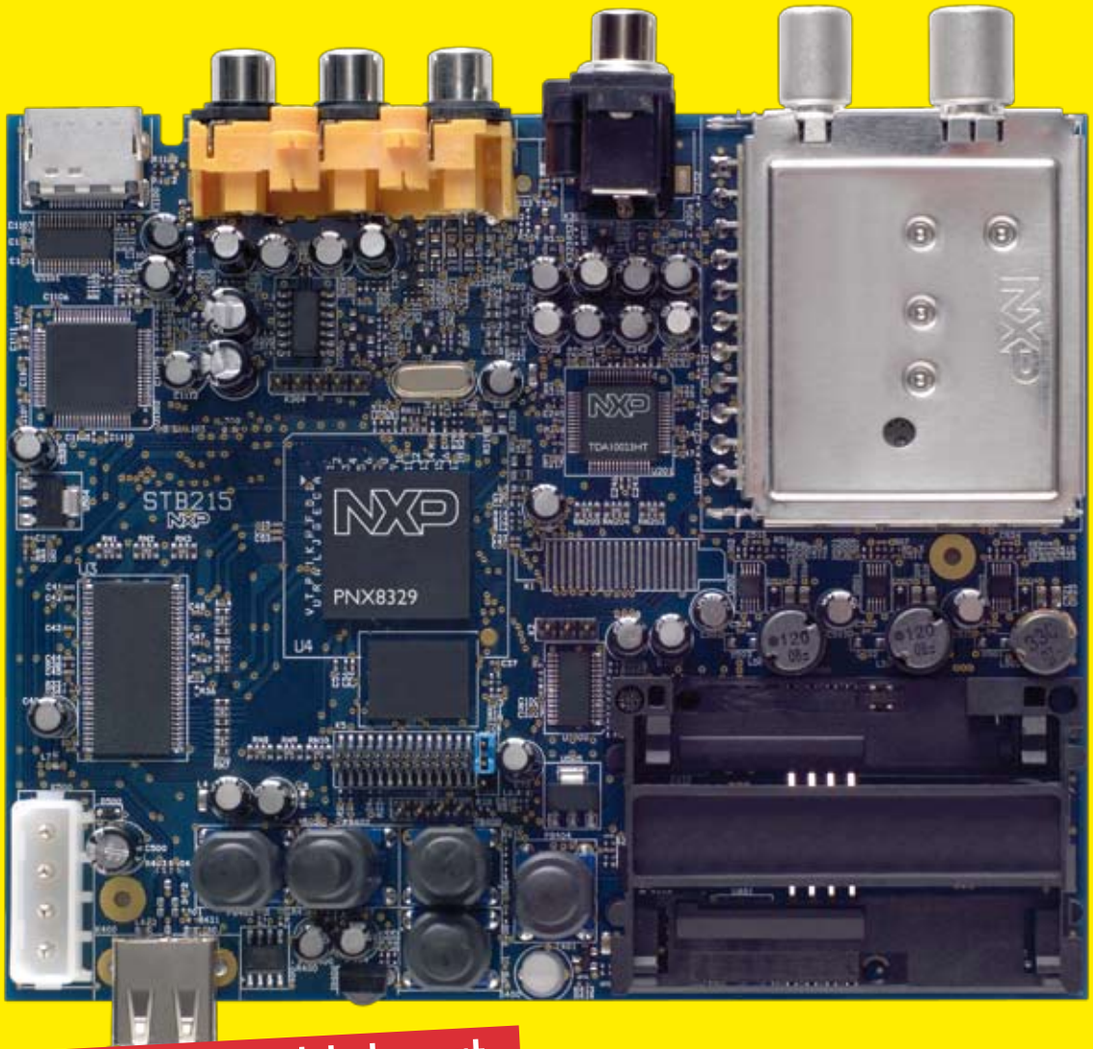

Reconstructie chipkaart

De **schokgolf** na de ontmanteling

De onderzoeksgroep van hoogleraar Bart Jacobs haalde in maart alle kranten nadat ze de geheime sleutel hadden gevonden van een cruciale chip. Die chip, de Mifare Classic, is de afgelopen tien jaar wereldwijd in een miljard pasjes verwerkt, van pasjes voor het openbaar vervoer tot toegangspasjes van overheidsgebouwen of militaire installaties. Een reconstructie van de sneeuwbal die op gang kwam na het eurekamoment. Over een vertegenwoordiger van de chipfabrikant die not amused was, de wekenlange spanning in het zenuwcentrum in het Huygensgebouw, en over twee AIVD'ers die onder de indruk zijn van de Nijmeegse vinding. "Dit is écht ernstig. De knop moet op rood."

Op vrijdag 7 maart om half vijf zitten tien mensen om tafel in een kamer van de afdeling Digital Security, de groep van hoogleraar Bart Jacobs die onderzoek doet naar onder meer de beveiliging van chipkaarten, stemcomputers en ov-passen. Niets in de kamer verraadt dat een kwartier later bij iedereen alle stoppen doorslaan, omdat na vier weken intensief geploeter de doorbraak op stapel staat. Het is zo'n typisch vrijdagmiddagmoment met de benen op tafel, Bart Jacobs is even binnengelopen om bij de werkbijen van zijn speciale eenheid – vijf studenten en vijf medewerkers – de voortgang te bespreken. Het gaat over koetjes en kalfjes. Ook het hiaat in de theorie waarop de groep zich al weken stuk bijt komt ter sprake. Gerhard, een van de studenten, gooit een balletje op: "Laten we het *readcommando* eens proberen."
De opmerking van Gerhard verwaait ogenschijnlijk, het gesprek komt op andere onderwerpen, een medewerker staat op het punt naar huis in Groningen te vertrekken. Ruben roept de suggestie van Gerhard in herinnering, zittend achter een laptop waar hij wat aan zit te klooien. "Het kost weinig moeite om even een programmaatje te runnen om Gerhards idee te checken." Ruben voegt de daad bij het woord, tuurt op zijn scherm en onderbreekt ruw de kabbelende conversatie. "Het klopt! Dit is het!" De hel barst los. Iedereen springt op om mee te kijken. "Laat zien, laat zien!" Er wordt een neptoegangspasje gemaakt, iedereen loopt de gang op om bij een interne deur het pasje uit te proberen. Gejuich stijgt op als de nepkaart inderdaad de deuren opent. "Het is gelukt. De kaart is gekloond."
Het eurekamoment zet een radar in gang die nog weken zal blijven draaien. Het is Bart Jacobs die na een kwartiertje feesten de zaak in beweging zet. Hij staat op om op zijn eigen kamer collegevoorzitter Roelof de Wijkerslooth in te lichten. "Ik haal hem erbij", zegt hij tot zijn groep. "We gaan de baas van de organisatie hierover inlichten. De knop moet op rood."

Target

De euforie in het zenuwcentrum van Digital Security was nooit ontstaan zonder de vinding van student Roel Verdult, die in januari de wegwerp-ov-chipkaart wist te ontmantelen. Daarna is de nog beter beveiligde abonnementskaart van de ov onder handen genomen. De chip daarin, de Mifare Classic, mag met recht een klassieker heten, want hij is in de tien jaar van zijn bestaan verwerkt in één miljard kaarten, onder meer in de pasjes die toegang bieden tot overheidsgebouwen en militaire complexen – *all over the world* – en in de kaartjes voor de Londense metro.
Wie de Mifare Classic kraakt, loopt het risico zélf een target te worden. Dat het zover wel eens zou kunnen komen, wordt duidelijk als Roel met een paar kompanen de sleutel van de chipkaart in zicht krijgt. Of beter: dénkt te krijgen, want als Roel midden februari overenthousiast de kamer van Bart binnenstormt om een vondst te melden, levert een eerste check een teleurstelling op. Roel had wel degelijk een serieuze fout ontdekt in het berichtenverkeer van de Mifare Classic, maar het bewijs is alleen rond te krijgen als je de geheime sleutel vindt, en díe had Roel nog niet in handen. "Maar dit is een geweldige stap in de goede richting", reageert Bart tegen Roel. "Je moet van die studentenkamer af, we gaan een eigen zenuwcentrum inrichten. Dit wordt bloedlink. De impact hiervan kan enorm worden."

'We gaan de baas van de organisatie hierover inlichten. De knop moet op rood'

Van links naar rechts: Wouter Teepe, Roel Verdult, Ruben Muijrers en Bart Jacobs / Foto: Bert Beelen

Het clubje van Roel wordt half februari omgevormd tot een speciale eenheid, met de inzet van een paar extra studenten en postdocs. Hun kamer gaat op slot, de hele groep wordt gemaand tot geheimhouding én het onderling e-mailverkeer wordt versleuteld. Als bewijs voor hun wetenschappelijke theorie kiezen ze het toegangspasje van de universiteit. De inzet is helder: wanneer dát pasje kan worden gekloond, is de theorie bewezen. En dat maakt vele pasjes met de Mifare Classic in één klap vatbaar voor namaak. Het enthousiasme groeit, kleine doorbraken volgen in de weken waarin de eenheid werkdagen maakt van vaak twaalf uur. De groep ruikt bloed. En terecht, blijkt op die bewuste vrijdag 7 maart. "Dit is een *once in a lifetime* kick", zegt een van de mensen als Bart Jacobs de deur uitloopt om De Wijkerslooth te bellen.

Meteen komen

Collegevoorzitter Roelof de Wijkerslooth loopt rond op een receptie in de Aula, na afloop van de oratie van UMC-hoogleraar Winette van der Graaf, als hij zijn mobiel checkt. Een sms'je en een voicemailbericht attenderen hem op pogingen van Bart Jacobs om hem te bereiken. Het is vijf uur als hij terugbelt. Hij kent zijn pappenheimers en de reputatie van Jacobs' groep als het gaat om het blootleggen van gevoelige beveiligingstechnieken.
"Roelof, volgens mij is er iets ernstigs aan de hand", zegt Bart. "Wat we nu hebben is tien keer groter dan onze vinding in januari. Ik stel voor dat je meteen komt kijken."
Roelof verlaat direct de receptie en fietst naar het Huygensgebouw. Als hij vijf minuten later binnenloopt, glundert de speciale eenheid nog na. Je drukt op de rode knop en in no time zit je met de hoogste baas aan tafel. Het kost de groep weinig moeite om de collegevoorzitter voor het verhaal te winnen. Hij krijgt gedemonstreerd hoe een bestaand pasje met een speciaal apparaatje wordt 'afgeluisterd', waarna een nieuw gekloond pasje alle deuren voor je opent. De Wijkerslooth is direct overtuigd en is zich in een nazit met Jacobs en medeonderzoeker Wouter Teepe bovendien bewust van de maatschappelijke gevolgen. Jacobs had in de voorbije weken alle tijd om een scenario te maken over 'wat te doen na code rood' en deelt zijn stappenplan met De Wijkerslooth. Eén: de rijksoverheid inlichten, in samenhang met de AIVD, twee: de fabrikant van de Mifare Classic op de hoogte stellen, met als derde stap het informeren van

de systeembouwers van de ov-chipkaart.
Toevallige bijkomstigheid is dat de bewuste chipmaker NXP heet, wereldwijd marktleider in de chiptechnologie en met bijna vierduizend werknemers de grootste commerciële werkgever in Nijmegen en omstreken. De Wijkerslooth hecht grote waarde aan zijn relatie met 'buurman' NXP, zeker omdat juist nu de samenwerking tussen het bedrijf en universiteit goed op gang begint te komen. De collegevoorzitter ziet zich voor een complexe opgave gesteld. Zonder deze relatie op de proef te stellen moeten de jongens van Jacobs, uit trots en academisch prestige, naar buiten kunnen treden met hun vinding. Bovendien moet worden gewaakt voor maatschappelijke onrust. De drie heren maken de afspraak om de vinding voorlopig stil te houden, om eerst de rijksoverheid de kans te geven maatregelen te nemen. Daarna is het de beurt aan Jacobs om de kennis te delen met NXP en in laatste instantie ook met het grote publiek.
Het is die vrijdag nog ongewis wanneer de kennis naar buiten kan. Wel is duidelijk dat de publieke informatie beknopt zal blijven, alle technische details – waarmee de universiteit ook als Academie kan glorieren – komen pas naar buiten in een paper voor een Europese conferentie in oktober. Jacobs kiest niet voor een conferentie in Amerika, omdat een nieuwe wet daar regelt dat bepaalde beveiligingsinformatie niet naar buiten mag komen. Op grond van die omstreden wet zijn al een aantal wetenschappers gearresteerd.


Roelof de Wijkerslooth
Foto: Peter van Aalst

Ongerustheid

Philippe Raets is als waarnemend secretaris-generaal de hoogste baas van het ministerie van Binnenlandse Zaken, en is thuis in Den Haag als hij om half acht vrijdagavond De Wijkerslooth aan de lijn krijgt. Dat Roelof in relatief korte tijd zo'n hoge ambtenaar thuis te pakken krijgt, hoeft niet te verbazen, gezien De Wijkerslooths verleden als topambtenaar in het Haagse. De collegevoorzitter brengt zijn informatie even accuraat als urgent voor het voetlicht, waarna ook Raets ongerust wordt. Sinds de perikelen met de ov-kaart weet ook hij dat de chip kwetsbaar is en niet het eeuwige leven heeft, maar de experts op het ministerie gaven de chip toch nog enige tijd van leven. Hoewel verrast, brengt hij Roelof nog tijdens het telefoongesprek zijn complimenten over voor de snelle en efficiënte ontmanteling en voor het feit dat hij de eerste is met wie de kennis wordt gedeeld.
Roelof noch Philippe zijn experts en achten beiden een serieuze check van het ministerie noodzakelijk. Raets rapporteert meteen die avond het explosieve nieuws aan de Algemene Inlichtingen en Veiligheidsdienst, die op zijn beurt de onderafdeling NBV in de startblokken zet. Die letters staan voor Nationaal Bureau voor Verbindingsbeveiliging, een afdeling die zich bezighoudt met het beveiligen van geheime overheidsinformatie.
Twee mannen van NBV worden aangewezen om de universiteit zo snel als mogelijk te bezoeken, als het even kan nog diezelfde vrijdagavond.
Eén van de NBV-mannen (namen van dit soort functionarissen zijn staatsgeheim) hangt om tien uur aan de lijn bij Jacobs: "De urgentie is duidelijk. De zaak is helder. Kunnen wij bij wijze van spreken vannacht nog langskomen?"
Jacobs is op zijn hoede: "Hoe weet ik eigenlijk dat u van de NBV bent?" In zijn organizer staat de naam van de hoogste NBV-baas, zodat hij een testje kan doen. "Wat is de naam van uw baas?"
De naam die volgt, is niet correct, waarna Jacobs schrikt, maar zich ook snel bewust is van een mogelijke omissie in zijn organizer. "En wat is de naam van de vorige NBV-baas?" De naam die dán volgt deugt, waarna de twee mannen tot de afspraak komen om zaterdagmiddag een controlemoment te organiseren voor de beveiligingsdienst. De ontmoeting, zaterdagmiddag tussen drie en vijf uur, loopt gesmeerd. De vragen van de twee veiligheidsmensen getuigen van grote deskundigheid, Verdult, Jacobs en Teepe aan de andere kant informeren adequaat en zijn geen moment ongerust over de robuustheid van hun vinding. Hun theorie staat als een huis en ook de NBV'ers schieten er geen gaten in. De twee mannen zijn geschokt over het relatieve gemak waarmee de Nijmegenaren de geheime sleutel van de Mifare Classic hebben ontfutseld en zetten in de loop van het weekend in Den Haag alle mensen op scherp. Raets wordt zondagochtend door de NBV geïnformeerd en stelt een lijst op met vervolgstappen. Alle secretarissen-generaal van ministeries krijgen een melding over het lek bij de toegang van hun gebouwen, evenals de bazen van andere instellingen en militaire installaties. De AIVD meldt het lek ook aan zijn zusterdiensten in de wereld, terwijl vroeg in het weekend minister Guusje ter Horst wordt geïnformeerd. Op haar beurt seint zij premier Balkenende in over de penibele veiligheidssituatie. Direct na het weekend valt in Den Haag het besluit om de Tweede Kamer per brief over de zaak te informeren, met daarin de aankondiging dat extra maatregelen volgen om gebouwen te beveiligen, nu de passen niet blijken te deugen. Extra complicatie in het Haagse is het debat in de Tweede Kamer over de ov-chipkaart, in de donderdag ná het weekend. De eerder gekraakte ov-kaart bevat dezelfde kwetsbare chip als de toegangspassen, wat het logisch maakt om de Kamer in elk geval vóór dat debat van de nieuwste bevindingen op de hoogte te stellen.

> **'De urgentie is duidelijk. De zaak is helder. Kunnen wij bij wijze van spreken vannacht nog langskomen?'**

Not amused

Terwijl in het weekend de gehele beveiligingsmachinerie in Den Haag op gang komt, weet NXP

De persconferentie op woensdag 12 maart in het Huygensgebouw

nog van niks. Het is al zondagavond als Hans de Jong, technisch architect van NXP, een telefoontje van Bart Jacobs krijgt. “We hebben een probleem ontdekt met de Mifare Classic. Ik raad je aan om morgen te komen kijken.” Over het wat en hoe krijgt De Jong aan de telefoon niks te horen, dat verneemt hij op maandagochtend, als hij om acht uur op de stoep staat bij het Huygensgebouw. De Jong, in gezelschap van NXP-overheidsliaison Thomas Grosfeld, is not amused. Verdult, Jacobs en Teepe vertellen alles wat ze op dat moment weten.

Ter verduidelijking organiseert De Jong daarna op maandagochtend nog een conferencecall, met inbreng van Wouter Teepe en enkele extra NXP-specialisten. De informatie is genoeg om ook in het bedrijf aan de noodrem te trekken. De Jong informeert maandag rond het middaguur Fred Rausch, directeur Nederland van NXP en die reageert hetzelfde als de eerste man van het ministerie: niet écht verbaasd omdat een tien jaar oude chip zijn langste tijd heeft gehad, maar wel onder de indruk van het tempo en de manier waarop Jacobs en zijn mannen de chip hebben ontmaskerd. Het bedrijf staat die maandag voor de klus al zijn grote klanten in de wereld te bellen met het slechte nieuws. De reputatie van NXP krijgt een knauw, want de reacties zijn zoals te voorzien: ze worden er niet vrolijk van.

Pas laat die maandag wordt het alle betrokkenen helder dat Ter Horst op woensdag de Tweede Kamer zal informeren. Op de universiteit komt op dinsdag in snel tempo de communicatietrein op gang, nadat universiteitswoordvoerder Willem Hooglugt door Jacobs om half tien nader over de bevindingen wordt geïnformeerd. Met het ministerie worden de klokken gelijk gezet en volgt afstemming over de naar buiten te brengen informatie. Het besluit is om op woensdag laat in de middag een persconferentie te beleggen, een tamelijk unieke gebeurtenis op de universiteit, waar Jacobs de bevinding zal toelichten. Keurig volgens afspraak gaan de uitnodigingen voor die conferentie en het persbericht pas de deur uit nadat de Kamer door de minister op de hoogte is gesteld. Vrijwel direct nadat de Kamer de brief ontvangt, op woensdag 11 uur, verschijnen de eerste berichten op de nieuwssites. De vinding wordt een mediahype, waarbij links en rechts nog wat olie op het vuur wordt gegooid. *De Telegraaf* tekent uit de mond van een deskundige op dat ‘het voor kwaadwillenden nu echt gemakkelijk is’ toegang te krijgen tot onder meer de militaire objecten. *De Pers* kopt later die dag: ‘Hacker opent kazerne’.

Philippe Raets
Foto: Ministerie Binnenlandse Zaken

Perslawine

Terwijl dinsdagmiddag de universiteit en het ministerie druk zijn met hun persberichten, belt Hans de Jong om aan Bart Jacobs het finale NXP-oordeel te melden. “Wij bevestigen je analyse en complimenteren je met het bereikte resultaat”, zegt De Jong. Pas in dát gesprek verneemt De Jong dat de dag erop het publiek en de Tweede Kamer worden geïnformeerd. Als NXP daarna de eerste versie van de persverklaring van de onderzoeksgroep onder ogen krijgt, is de reactie negatief. “Een opgeklopt en dramatisch verhaal,” reageert NXP-baas Fred Rausch, “dat niet past binnen de academische traditie om alleen juiste en objectieve informatie naar buiten te brengen.” Nog net weet het bedrijf in de definitieve versie van het persbericht de zinsnede te krijgen dat volgens NXP ‘tegenmaatregelen mogelijk zijn die het risico aanzienlijk beperken’.

Een voor NXP ongelukkige passage in de brief aan de Tweede Kamer maakt de stemming in het bedrijf er niet beter op. Ter Horst schrijft: ‘Deze chip wordt gebruikt in naar schatting 2 miljoen toegangspassen in Nederland en 1 miljard passen wereldwijd.’ Een pijnlijke misser, oordeelt Rausch, te meer daar alle media die getallen klakkeloos overnemen. De waarheid is dat de Mifare Classic in de afgelopen tien jaar één miljard keer is verkocht, ook voor banale toepassingen in kantine- en parkeerpasjes. En een groot deel van die miljard passen zal inmiddels uit de roulatie zijn.

Door de voor het bedrijf al te

Fred Rausch / Foto: Bert Beelen

snelle ontwikkelingen blijven allerlei kanttekeningen die het bedrijf graag had willen plaatsen buiten beeld. Bijvoorbeeld dat het helemaal niet zo gek is dat een tien jaar oude chip wordt gekraakt en dat het eigenlijk een compliment is aan NXP dat tien uiterst knappe universitaire koppen nog wekenlang moesten broeden om de geheimen te vinden. En onderbelicht blijft de boodschap van NXP dat elk beveiligingssysteem nu eenmaal zijn zwakke plekken heeft, en dat een toegangspas – met welke chip ook uitgerust – slecht een klein onderdeel is in een lange keten van beveiligingsmaatregelen. NXP ziet er geen heil in om de pers alsnog met zijn boodschap te bestoken. Alles ligt nu toch al op straat, is de gedachte. Gelaten laat NXP de perslawine, woensdag op alle journaals en donderdag in alle kranten, over zich heen komen.

Fles wijn

Vrijdag 14 maart, de dag nadat alle kranten het nieuws over de onveilige toegangspasjes melden, komt in een zaaltje op de tweede verdieping van het bestuursgebouw een bont gezelschap bij elkaar voor een goed gesprek. Bart Jacobs is er, die de drukste week van zijn leven achter de rug heeft, samen met de directeur van de bètafaculteit. Roelof de Wijkerslooth schuift aan, nog onder de indruk van de snel werkende Haagse machinerie. Hij wil geen kwaad woord meer horen over verkokerde ministeries en lakse ambtenaren. Ook Fred Rausch, Hans de Jong en Thomas Grosfeld zijn

Gelaten laat NXP de perslawine, woensdag op alle journaals en donderdag in alle kranten, over zich heen komen

present, niet te flauw om Bart Jacobs en de ook aanwezige Wouter Teepe te fêteren met een goede fles wijn. Jacobs is verrast met het geschenk, wetende dat hij binnen NXP minder populair is dan daarbuiten.

Bart Jacobs verrast de Nijmeegse chipfabrikant met het nieuwtje dat de onderzoekers alweer een stap verder zijn met de ontmanteling van de chip. Rausch krijgt nu slechts de grote lijnen van de vinding geschetst, wat het voor hem lastig maakt om de claim goed op waarde te kunnen schatten. Op tafel komt de kwestie om over en weer tot meer openheid te komen. Omdat de eigen kennis waarde vertegenwoordigt, suggereert de universiteit een investering van NXP voor nadere informatie over de recente vindingen. De drie NXP'ers vinden dit geen goede weg. Los van de concrete zaak doet het bedrijf – niet voor het eerst – het voorstel aan Jacobs om een NDA te tekenen, zodat bedrijf en universiteit zich samen kunnen buigen over beveiliging van toekomstige producten. "Ik heb met onderzoekers uit Leuven ook een NDA getekend", zegt Rausch, "en dat werkt aan beide kanten uitstekend. Wij kunnen dan veel opener zijn over de werking van de chips."

Voor Jacobs is zo'n *non-disclosure agreement* een gruwel. Zo'n contract van onderzoekers en commerciële partijen regelt dat bepaalde kennis wordt gedeeld, maar dat nader te omschrijven gevoelige informatie niet naar buiten komt. "Ik moet leven van mijn publicaties," schetst Jacobs zijn positie. "Ik kan niet bij alles wat ik schrijf gaan nadenken over afspraken die ik met Jan en alleman heb gemaakt over informatie die geheim moet blijven."

Belangrijker nog vindt Jacobs zijn maatschappelijke missie om het publiek open te kunnen informeren over wat er aan de hand is in de automatiseringswereld die doordringt in steeds meer terreinen van ieders leven. "Er zijn al zo weinig mensen met verstand van zaken die zonder last en ruggespraak over deze materie kunnen spreken", houdt Jacobs het gehoor voor, "want bijna iedereen in het veld heeft een NDA getekend. Zulke NDA's worden politiek ingezet zodat ik verder mijn mond moet houden."

Jacobs en Teepe keren met hun fles wijn terug naar het Huygensgebouw. "Die gaan we soldaat maken met onze boevenbende", lacht Jacobs bij het weggaan. Nauwelijks één week later, op donderdag 20 maart, kan het tweetal nóg een keer zijn zegeningen tellen op de publieke tribune van de Tweede Kamer. GroenLinks heeft, vrijwel direct nadat minister Ter Horst haar brief aan de Kamer zond, om dit spoeddebat gevraagd. De parlementariërs loven de minister om haar daadkrachtige aanpak en vragen om onderzoek naar een juridische claim tegen NXP. Ter Horst beseft dat zij een deel van de aan haar gerichte complimenten mag doorspelen aan de Nijmeegse universiteit en na afloop schiet zij Jacobs en Teepe aan. Goed dat jullie de informatie eerst met ons hebben willen delen, zegt Ter Horst, "en bedankt voor de prettige samenwerking". Als voormalig burgemeester van Nijmegen wil ze ook dít gezegd hebben: "Het is erg leuk dat uitgerekend de Nijmeegse universiteit hiermee in het nieuws komt." x

Tekst: Paul van den Broek