Ir. Eric Luiijf, grondlegger van het militaire internet in Nederland

Militaire verbindingen waren er veel eerder dan ‘eerste internetconnectie’ van het CWI

Eric Luiijf is behalve internetbouwer van het eerste uur voor defensieonderzoek, ook ’s lands meest gerenommeerde cyberveiligheidsspecialist. Uiteraard remt geheimhouding het vraaggesprek in Scheveningen. Maar het is boeiend, over de prachtige beginjaren tot en met de spionage vandaag de dag.

C.V.
1952 geboren te Amsterdam
1969 – 1975 TU Delft, studie Wiskunde
1975 – 1976 Koninklijke Marine
1976 – heden Verschillende functies Physisch Laboratorium TNO, later Fysisch en Elektronisch Laboratorium TNO (FEL-TNO), waaronder tot 1995 afdelingsmanager computer- en netwerkvoorzieningen.
1995 – heden Principal consultant Critical (Information) Infrastructure Protection en Cyber Operations bij TNO Networked Operations)
Verder voorheen ook werkzaam voor:
Netherlands Centre for Protection of National Infrastructure (CPNI.NL)
National Infrastructure against CyberCrime (NICC)
Clingendael Centre for Strategic Studies (CCSS)

Eric Luiijf was vanaf de jaren tachtig verantwoordelijk voor de Arpanet-, later internetkoppeling van FEL-TNO, onderdeel van de defensietak van TNO. Hij nam al vroeg deel in de internationale coördinatie. Sinds 1995 werkt hij aan projecten voor bescherming van vitale (informatie)infrastructuren voor de Nederlandse overheid, bedrijfsleven en de EU.
Bij het vraaggesprek hoort een rondleiding door het boeiende Museum Waalsdorp dat toont dat ook Nederland goed kon spionieren en vooral met de marine zijn mannetje internationaal stond.

Het Centrum voor Wiskunde en Informatica (CWI), gelauwerd voor de eerste internetverbinding, erkent dat de eerste echte Europese internetverbindingen militair waren. Ook in Nederland?

"Londen was het eerste grote internetknooppunt in Europa. Sinds juli 1973 lag er een verbinding tussen het militaire Arpanet in Amerika en het University College London (UCL) als Europees knooppunt. Arpa of Darpa – ze wisselden hun naam nog wel eens in die tijd - het onderzoeksagentschap van het Pentagon, sponsorde deze internationale uitloper aan het Arpanet. Behalve naar UCL betaalde Arpa ook de aansluiting van defensieresearchinstituten in Ottawa (Canada), Noorwegen, het Royal Signal Research Establishment (RSRE) in Engeland - het latere Defence Research Agency - en het NATO Shape Technical Centre (STC) in Den Haag. Dat was dus de eerste verbinding in Nederland.
Het netwerk had uitlopers met inbelverbindingen naar ondermeer IABG in Duitsland en een defensieresearchinstituut in Italië. Op een kaartje uit 1977 en later een kaartje uit 1982 van Jon Postel is zichtbaar hoe Arpanet toen was opgebouwd."

De worstelingen voor die eerste verbinding naar Europa heeft professor Peter Kirstein uitgebreid opgeschreven in een onderzoeksdocument (later korter). Hij spreekt over SATnet, een netwerk dat via satellieten liep. De Britse onderzoeksgemeenschap had geen interesse en hij kreeg nauwelijks geld los. Vreemd?

"Het was inderdaad ontzettend pionieren voor Kirstein. Het is goed dat Darpa, geholpen door de National Science Foundation (NSF) en Nasa in de VS, bijgesprongen hebben voor die eerste verbindingen met Europa. Hier ging al IP-verkeer overheen, maar met een Terminal Interface Protocol, net genoeg voor eenvoudig bulletin board gebruik.
De knooppunten waren gebaseerd op BBN Butterflies [Bolt, Beranek, Newman], een voorloper van wat nu routers zijn. Daar is, vanaf 1967, een hele geschiedenis aan verbonden. Regelmatig moesten deze dozen synchroon opgewaardeerd worden. Internationale afstemming was vereist. Kirstein heeft voor de internationale coördinatie de International Collaboration Board (ICB) opgericht, die net als IETF [algemeen internetstandaardisatieorgaan] een relatie had met de Internet Architecture Board."

Waarom deden er zo weinig landen mee, enkel computerspecialisten van de nationale onderzoeksinstituten voor Defensie in Duitsland, Denemarken, Engeland en Nederland, plus de Navo en Arpa?

"Rond 1975 begon de ICB met Peter Kirstein als voorzitter. Hij was geboren in Duitsland, in Engeland opgegroeid en in Amerika aan de University van Berkeley afgestudeerd bij de Arpanet ontwikkelgroep. Dus hij had korte lijnen en werd vertrouwd bij Arpanet.
Een beperkt aantal defensieresearchinstituten was geïnteresseerd in de vernieuwende concepten van Arpanet. Officieel lag de focus van de Navo en de lidstaten op de oude telefoniestandaarden en op ISO/OSI dat net in ontwikkeling was.
Arpanet kwam voort uit wat de 'internetanarchie' werd genoemd. De ICB had geen enkele formele status bij de deelnemende landen en de Navo. Dat leverde nogal eens vragen op als men de ICB probeerde te plaatsen of vinden.

Het Physisch Laboratorium TNO, later Fysisch en Elektronisch Laboratorium of TNO-FEL, werd rond 1983 uitgenodigd om deel te nemen aan de ICB. De eerste Nederlandse ICB-vertegenwoordiger was Dick Fikkert, die onderhandelde voor de Arpanetverbinding naar TNO. Hij werd opgevolgd door René van Assem en vanaf eind jaren negentig was ik de ICB-vertegenwoordiger."

Hoe waren jullie verbonden?

"Vanaf circa 1985 gebruikten we in eerste instantie een terminallijn aan het Arpanet met BBN-technologie bij onze Navo-buurman STC. Vooral om te communiceren via bulletin boards. Rond die tijd was dat feitelijk illegaal omdat de nationale PTT's wettelijk het alleenrecht hadden voor uitwisseling van tekst met andere landen, nog via de telex.
De Darpa-vertegenwoordiger in de ICB probeerde Darpa-geld te vinden om ook TNO te voorzien van een directe BBN Butterflypoort. De eerste stap in dat proces was een zogenaamde B-klasse adres te krijgen. Dat nam lang in beslag, maar is uiteindelijk gelukt. Het was 134.203.0.0 waarmee we in principe ruim 65.000 systemen rechtstreeks op het Arpanet konden ontsluiten."

Naar STC en later TNO lag dus de eerste echte internetverbinding in Nederland. Dus niet in 1988 naar het CWI?

"Ja, dat was de eerste. Om niet mee te hoeven te betalen aan de dure verbinding van STC naar Engeland koppelden we rond 1989 ons Arpanet-segment, behalve aan STC, ook aan EUnet/NLnet met UUCP; de voorloper van internet in Europa. Dat was moeizaam omdat Piet Beertema niets op had met defensie en defensieresearch en ons IP-adres niet wilde registreren. Uiteindelijk liet hij liet het toch doorgaan.
Ons verkeer naar de Engelse en Canadese defensiecollega's ging via STC, het andere Europese netwerkverkeer van TNO werd via NLnet gerouteerd. Daarmee hadden wij een directe en indirecte lijn met het internet en gaven we – in het begin illegaal voor NLnet – een back-up aan STC."

Hoe lang is die illegale verbinding blijven bestaan?

"Enkele jaren, totdat STC budget vrij kon maken voor internet, zoals gezegd een communicatietechnologie die Navo formeel niet erkende. In 1993 kregen we een vaste 64 Kb/s huurlijn met NLnet waarvan de capaciteit daarna met enige regelmaat werd uitgebreid.
Jaarlijkse kosten voor internet begin jaren negentig waren voor TNO 85.000 gulden, een flink bedrag."

Hoe werd het internationaal geregeld?

"In 1992 betaalden NSF, Nasa en Darpa ieder voor 256 kbps bandbreedte van wat de 'fat pipe' tussen de VS en Europa heette. Voor de directe koppeling met Londen of met een collega defensie-instituut betaalde elke organisatie zelf de rekening of deelde dat met zijn collega. Soms betaalde Darpa de rekening in het kader van internationale projecten en samenwerking.
Slimme software van de UCL-groep zorgde in de loop van de jaren '90 dat niet gebruikte bandbreedte door de andere fat pipe-partijen gebruikt kon worden. Kirstein was continu in de weer om om de beurt NSF, Nasa en Darpa te wijzen op hun piekgebruik en de noodzaak om op basis van goed vaderschap hun gecontracteerde bandbreedte uit te breiden."

U was er als jonkie al vroeg bij. Bijzondere herinneringen?

"De ICB-bijeenkomsten in de Verenigde Staten werden bij toerbeurt gehouden bij Darpa en ISI East in Washington DC en bij ISI West in Marina del Rey Californië. Dat betekende persoonlijke contacten met

de godfathers en andere sleutelfiguren van het internet, zoals Bob Kahn, Vint Cerf, Debra Deutsch (BBN) en Paul Mockapatris (DNS ontwerper). Onderzoekers kwamen uitleg geven over bijvoorbeeld routingontwikkelingen zoals met BBN en DNS, over experimenten zoals XBone van Joe Touch, VPNs, S/MIME en XML-Secure.
We hadden discussies over de vraag of je genoeg zekerheden kon inbouwen voor militair verkeer in een periode dat de ISO/OSI standaarden, ook voor e-mail, opgang deden in de Navo. We hadden twintig jaar geleden ook al discussies over IP-versie 6, testten die zelfs al. Nu is het nog niet ingevoerd.

Ook waren er discussies over fouten in de TCP protocollaag op het moment dat de traagheid van de fysieke verbindingen niet meer de bottleneck in de communicatie vormde. De doorvoersnelheid werd daardoor beperkt."

De aartsvaders ook ontmoet?

"Het meest bijzonder was de ontmoeting met de fameuze John Postel, jarenlang ongeveer de persoonlijke beheerder van de internetadressen, later via de organisatie Iana. Ik reed eens met hem mee naar een vergadering. Op de vloer van zijn Amerikaanse slee lag een hele laag sigarettenpeuken. Een kettingroker die alleen maar met internet in de weer was en daar aan één stuk door over sprak. Heel bijzondere man.
Samen uit eten was een feest.
We zijn met de hele ICB nog een keer bij Vint Cerf thuis uitgenodigd. Dat zijn de onvergetelijke herinneringen. Vooral toen hij een 'catwalkshow' organiseerde waarin hij zijn vele unieke buitengewoon hoogleraartoga's van over de hele wereld showde."

Het CWI verhaalde over verkeer van seismische metingen van de Salt-wapenakkoorden via hun poorten. Moest dat niet via het militaire net?

"Dat is me volslagen onbekend, maar dat kan wel via het researchnet van NSF en het seismisch instituut in Amerika zijn gegaan. Dat was niet zo strikt gescheiden en liep die dagen door elkaar. Beveiliging van militair verkeer speelde eigenlijk nog niet zo."

Geen strikte scheidingen en beveiliging? Jullie hadden toch een eigen .mil domein?

"Het topdomein .mil was van Defensie in Amerika. De ICB had een eigen topdomein in beheer: .int. Feitelijk viel daar enkel Navo onder. We hebben wel geprobeerd om de Europese Commissie te bewegen om een .int internetdomeinnaam te nemen. In Brussel was men toen echter niet geïnteresseerd in Arpanet.
In die tijd waren de standaardisatieoorlogen belangrijker, eerst met domeinnamen zoals .gb versus .uk, later met de vanuit Brussel opgelegde ISO/OSI-standaarden X.400/X.500 versus SMTP met S/MIME."

Bestaat er nog zoiets als een apart Milnet?

"Natuurlijk, helemaal separaat van het andere internetverkeer. Er stat, wat ik noem 'een hele grote wasstraat' tussen Milnet en het gewone internet met een groot aantal firewalls en gateways in serie opgesteld om het verkeer veilig over te dragen."

Zit TNO op Milnet?

"Nee, absoluut niet. Het is enkel voor de Amerikaanse Defensie. Maar er zijn wel aparte researchnetwerken voor defensie zoals het Combined Federated Battle Laboratories Network oftewel het CFBLNet. Rond 1995 ontsloot TNO-FEL wel haar internetverbindingen via terminals voor researchafdelingen van het ministerie van Defensie."

Hebben militairen een beter internet dan wij?

“We hebben in ICB-verband wel altijd de nieuwste technologie getest om het netwerk robuuster te maken. Die technologie komt dan na verloop van tijd ook civiel beschikbaar.
We hebben bijvoorbeeld een test gedaan om via lagen in routers een tweede prioritair netwerk op te zetten, bijvoorbeeld voor noodsituaties als overstromingen. Dan kun je een deel van de communicatiecapaciteit reserveren voor crisismanagementverkeer.”

Nooit van gehoord…

“Het is ook niets geworden, maar veel van die experimenten waren bijzonder.”

Wetenschapsnetten zoals Surfnet waren in 1992/1993 wel klaar met de Osi-standaarden, jullie niet. Vanwege de grotere veiligheid van de Osi-standaarden?

“Die discussie speelde binnen de Navo zeker tot midden jaren negentig. Inderdaad vanwege veiligheid en stabiliteit. Die hobbyisten aan de internetkant waren wel prima, maar de Navo en lidstaten waren de klassieke PTT’s gewend. Dat waren met de staten verbonden organisaties en daarom vertrouwd en veilig.
Het heeft dus even geduurd voordat men geheel vertrouwd raakte met TCP/IP. Hier bij TNO waren we de eersten die een aantal gateways gebruikten voor informatiestromen tussen de verschillende local area netwerkstandaarden: XNS, DECnet en native OSI-stack. Omdat onze leveranciers ook TCP/IP gateways ging leveren, zagen we dat als de lijmlaag tussen het mainframe van Control Data, onze Digital Equipment en CAD-CAM systemen. Vreemd genoeg werd de TCP/IP-wereld pas als laatste ondersteund door de pc/server systemen van Novell.”

Wat deden jullie zelf met die internetverbinding?

“Eerst bulletinboardverkeer, later werd dat vooral e-mail verkeer en uitwisselen van meetdata via ftp. Inhoudelijk voornamelijk het analyseren van technische communicatieproblemen en zoeken naar oplossingen. En in ICB-verband experimenten met de infrastructuur, zoals de eerste pogingen om teleconferenties te houden. Veel multimedia-experimenten via internet en multicasting verliepen teleurstellend door ‘jitter’; lange transporttijden omdat de gedeelde internetverbindingen nog weinig bandbreedte kenden en tussenschakels in het netwerk de multicasting blokkeerden.
Met drie beelden per seconde video bereikte je niet veel. Toch vormden die experimenten de basis voor de huidige toepassingen als Skype en Voice-over-IP over de veel sneller geworden netwerken.
Daarna verschoof de aandacht van de ICB naar informatie- en netwerkbeveiliging van de vaak trage en niet altijd betrouwbare verbindingen.”

Ook veel met simulatie via netwerken gedaan?

“In 1995 hebben we in de Statenhal van het Congresgebouw ruim dertig simulatoren gekoppeld over zware ISDN en internetverbindingen voor een grote virtuele oefening op een kunstmatig gevechtsterrein. F16-simulatoren in Orlando vlogen boven het gevechtsveld. De F16-vliegers zagen in hun cockpits hetzelfde terrein als bijvoorbeeld de tankbestuurders in Den Haag en F16-simulatoren elders in Nederland.
De koppeling met Amerika ging via het Defense Simulation Internet (DSI), dat over de hele wereld simulatoren van militaire platformen als vliegtuigen, tanks en schepen met toen hoge bitsnelheden verbond.
Onze toegang tot dat netwerk was op de Amerikaanse luchtmachtbasis Ramstein in Duitsland, via drie parallel werkende ISDN routers. KPN en Deutsche Telekom hadden grote moeite met onze aanvraag, want ISDN-lijnen werden standaard als spraaklijnen geconfigureerd.”

Wat was er bijzonder aan DSInet?

"We werkten met IP versie 5, ook wel ST 2. Ik denk dat wij dat als enigen in Nederland hebben gebruikt. Het bood prioriteiten en gegarandeerde, vooraf te reserveren, bandbreedte voor de koppeling van simulatoren. Wel nodig als je toestellen in de lucht moet houden en niet schokkend in beeld wil zien omdat de IP-pakketten onregelmatig binnen komen. Dat werkte, gegeven de stand van de technologie toen, uitstekend."

Was er veel overleg over beveiliging?

"Paul Overbeek, helaas vroeg overleden, was een topper in informatiebeveiliging. Hij ontdekte dat je zonder bevoegd te zijn informatie uit de eerste versies van TCP/IP kon halen. Dat soort tekortkomingen hebben we verholpen.
ICB-leden namen deel aan de beveiligingssessies van Darpa. Die gingen eind jaren negentig ondermeer over Next Generation Internet of Internet2. Er was ook veel internationaal enthousiasme binnen de ICB over een onderzoeksvoorstel voor netwerkbeveiliging bij de Canadese collega's. Daaruit is nog Entrust ontstaan, een van 's werelds meest gerenommeerde beveiligingsbedrijven. Eigenaar van vele patenten en steeds medegastheer voor de ICB als we weer in Ottawa vergaderden."

Dat Internet2 is er nooit gekomen. Zouden we dan wel veilig geweest zijn?

"De toegankelijkheid tot het netwerk zou wat minder makkelijk geworden zijn. Maar Internet2 ging vooral over bandbreedte en veel hogere snelheden met nieuwe protocollen over glasvezel. Deze benutting was en is niet optimaal.
Internet2 kan alsnog tot stand komen, maar dan moet er wel een slag gemaakt worden. Het is nu immers heel moeilijk om nieuwe elementen aan internet toe te voegen of iets te vervangen. Het internet wordt nu zo breed gebruikt. Vroeger kon je met de technici afspreken: nu gaan we ervoor en maken een overstap naar een nieuwe versie of implementatie. Dat kan nu moeilijk. Zie maar hoe veel pijn de overgang naar IPv6 veroorzaakt."

Hoe draagt TNO operationeel bij aan Defensietaken, zoals ooit begonnen in Libanon en nu in Mali?

"We doen langere termijnonderzoek voor Defensie en geven soms directe operationele ondersteuning. Details kan ik niet vertellen. Sommige collega's zijn vrijwillig reserveofficier. Ik heb respect voor die collega's, die dan drie maanden in zo'n zeecontainer huizen in het stof van Afghanistan om daar hun kennis in praktijk te brengen."

De NSA en AIVD staan in het brandpunt van belangstelling, maar 15 jaar geleden hadden we Echelon al. Hoe volgden jullie de onthullingen over spionage toen en nu?

"Je had Echelon, maar ook Frenchelon, de elektronische spionage door de Fransen. Dat is meer onder de radar gebleven. Nu nog ligt het accent in de media op Amerika en Engeland, maar vergeet niet dat alle grote staten uitgebreid spioneren. Kijk bijvoorbeeld op Cryptome wat er her en der aan spullen staat om af te luisteren. Dat is een wereld op zich.
Het BSI in Duitsland toonde een aantal jaren geleden foto's van gemodificeerde mobiele telefoons waarmee andere staten 'captains of industry' afluisterden. Fransen hebben in de beginperiode van GSM de encryptie tussen antenne en telefoon gewoon uitgezet. Spionage is van alle tijden en van alle kanten."

TNO krijgt uiteraard onderzoeksopdrachten naar bijvoorbeeld lekken in hardware; de achterdeurtjes?

"Daar kan ik niets anders over zeggen dan dat TNO in de periode van de koude oorlog werkte aan opsporings- en decoderingsapparatuur. [zie Museum Waalsdorp]."

Nederlandse operators werken heel veel met Chinese apparatuur, die in de VS wordt geweigerd uit angst voor achterdeurtjes. Hebben jullie deze apparatuur onderzocht?

"Niet dat ik weet. Voor dergelijke zaken moet ik je verwijzen naar het NBV, het Nationaal Bureau Verbindingsbeveiliging, een onderdeel van de AIVD dat mede betaald wordt door Defensie, Binnenlandse - en Buitenlandse Zaken. Ze testen encryptie, vaardigen richtlijnen uit voor encryptie, evalueren apparatuur tot op bit- en uitstralingsniveau, omgevingsfactoren, risico's voor de staatsgevoelige communicatie."

Verraste de mededeling u dat de encryptie van het zeer betrouwbaar geachte beveiligingsbedrijf RSA op de burelen van de NSA in Virginia ligt?

"Nee. Maar de sterkte van 'civiel' beschikbare encryptie was altijd een internationaal discussiepunt. Zelfs de eerste PGP-versies bleken niet geheel veilig, want ze lekten sleutelinformatie.
Van een Amerikaanse collega kreeg ik onderhands een snelle softwarematige DES-versie. Enkele weken later legde de NSA een exportverbod op voor die code. Natuurlijk gebruikten we die code in ons mainframe voor de bescherming van laag gevoelige informatie."

U doet veel geheime dingen?

"Deze locatie waar je nu binnen bent, is door de overheid aangewezen als Verboden Plaats in het kader van de Wet op de Staatsgeheimen. Over gevoelige zaken praten we niet. Andere discussies kunnen we wel in alle openheid voeren."

Is er nog open uitwisseling tussen militairen en de IETF standaardisatie? Gaat u naar de bijeenkomsten van de IETF?

"Ik zou persoonlijk wel willen, maar er is geen geld meer voor. Defensiebezuinigingen hebben ook hun effect. In 2002 is de ICB opgeheven, maar er zijn wel contacten tussen Navo-werkgroepen en de IETF. Standaardisatie wordt natuurlijk op de voet gevolgd."

Wat voor soort onderzoek doet u nu?

"Veel civiele veiligheidsonderwerpen, zoals naar vitale infrastructuren. Modelvorming en empirische analyse van afhankelijkheden tussen vitale infrastructuren. Ook de ICT-kwetsbaarheid van procescontrolesystemen en dreigingen voor smart grids in energievoorziening.
We ontwikkelen 'what if' analysemogelijkheden op basis van gekoppelde vitale infrastructuursimulatoren. Dat helpt het crisismanagement bij mogelijke uitval van vitale infrastructuur. Verder heb ik een groot aantal nationale cyber securitystrategieën geanalyseerd en meegeschreven aan het Nato Cyber Security Framework Manual.
Mijn collega's en ik hielpen mee met de opzet van good practices voor Europese beleidsmakers op het gebied van bescherming van vitale infrastructuur. Ook schrijf en werk ik mee aan cybersecurity en andere scenario's voor de nationale risicobeoordeling."

U schreef wetenschappelijke en populaire publicaties, doet lezingen en interviews om de bewustwording te verhogen over de kwetsbaarheid van vitale infrastructuur bij overheid, bedrijfsleven en bevolking. Heeft dat genoeg effect?

"De onderlinge verwevenheid van vitale infrastructuur heeft aandacht, maar wordt steeds complexer mede doordat informatie- en communicatietechnologie daar steeds dieper deel van uitmaakt. Aandacht voor de kwetsbaarheid van het Nederlandse deel van het internet is zeker opgepakt na de KWINTrapportage van Jaap van Till in 2001.
Het blijft echter een continue discussie. Er gaan zoveel verschillende vitale diensten over het internet terwijl dat er eigenlijk niet voor gemaakt is en ook niet zo geschikt voor is. Ook internet basisprincipes worden wel eens vergeten."

Zoals?

"Het ontwerp van internet is gericht op het doordraaien van communicatie via alternatieve routes als er een belangrijk knooppunt uitvalt. Dat werkt als je met een zuiver internet IP-adres aankomt. Gebruik je echter een URL als www.museumwaalsdorp.nl dan ben je erg afhankelijk van DNS-servers die toch een 'single point of failure' vormen. Er is wel een laagsgewijze redundantie ingebouwd voor kortstondige storingen, maar die is niet altijd voldoende om de boel draaiende te houden bij een gerichte cyberaanval op een belangrijke DNS-server."

Dus internet kan plat?

"Met het echec van KPNQwest bleken DNS-voorzieningen van .nl en enkele andere landen alleen aan dat netwerk gekoppeld te zijn. We kropen toen als Nederlands internet door het oog van de naald.
Op 11 september 2001 viel ook het topleveldomein van enkele landen uit, omdat er te veel bij één partij en op één locatie in Amerika was belegd.
Het risico van uitval van vitale infrastructuur door een ontregelde cyberinfrastructuur neemt toe. Steeds meer vitale systemen en diensten worden aan het internet gekoppeld. Deregulering en nieuwe eisen zorgen er bijvoorbeeld voor dat bedrijven uit de vitale infrastructuur moeten koppelen aan internet omdat ze productie-informatie uit procescontrolesystemen naar moeten buiten brengen. Er ligt dan dus een risicovolle verbinding met systemen voor procescontrole van bijvoorbeeld de energiebedrijven."

Het virus Stuxnet bracht ons bij de les?

"Dat was niet het eerste en enige incident. Er zijn meer incidenten geweest waaruit blijkt dat vitale infrastructuur niet allemaal even veilig gekoppeld wordt. In Amerika en Australië gelden rapportageplichten bij uitval, dus daar horen we van een virus in de elektriciteitstransmissie of nucleaire centrales.
In Australië ging het helemaal mis met een transmission system operator voor elektriciteit. Het controlesysteem kon net op tijd losgekoppeld worden. In een groot Europees land heeft een hacker twee weken lang de elektriciteit van ruim 50 miljoen burgers op het spel weten te zetten. Dat is al weer een poos geleden… Nee, meer kan ik niet zeggen."

Toen KPN vorige jaar in kritiek vaarwater kwam door een hacker op de servers, werden TNO en u persoonlijk toen ingeschakeld?

"Nee. Op ICT-beveiligingsgebied heeft KPN zelf competente mensen."

Maar u bent toch in beveiliging en kwetsbaarheid al jaren de grootste autoriteit in Nederland, ofschoon minder bekend dan Ronald Prins van Fox-IT?

"Ja, waarschijnlijk wel, maar dat wil niet zeggen dat ik mij met de technische details bezig houdt. Collega's kennen die vaak beter, want je moet er de hele dag mee spelen. Vooral iets voor de jongere garde. Ik werk meer op het strategische en tactische niveau, maar moet wel de vertaling kunnen maken van het actuele technische niveau."

Strategisch belangrijk om de hackers aan de goede kant van de streep te trekken met een zak geld? Het is een hele dunne lijn…

"Hacking is inderdaad een hele dunne lijn. Je moet toch vaak eerst wat aan de 'foute kant' hebben gedaan voor je in beeld komt als een goede hacker. Ja, wij zoeken ook intensief naar dergelijke 'hobbyisten'. Maar we zijn daarin niet alleen actief. Ook Defensie en de politie zoeken naar mensen met dezelfde technische interesses."

Dus je moet de hackers tarten om voor een hoog salaris te gaan aan de goede kant van de lijn?

"Er liggen uitdagingen, ja. We zoeken vooral jongens en meisjes met een exploratieve geest. In de begintijd van het internet en in de tijd dat we hier van alles koppelden, haalden we ook de nodige lekken en fouten uit protocolimplementaties en besturingssystemen.
Het waren soms uitdagende en lange nachten en weekenden om fouten te verhelpen en misbruik te voorkomen. Het was leuk. Jammer is dat in elke nieuwe generatie ICT nog steeds dezelfde typen ontwerpfouten zitten: buffer overflows, gebrek aan controle op valide invoer, enzovoort."

Wat is er veranderd?

"Behalve dat we meer strategisch adviseren, is het terrein ook breder geworden. Zo kijken collega's ook naar de risico's van het gebruik van Twitter en andere sociale media. Anderzijds ook hoe autoriteiten die technologie tijdens evenementen of een crisis kunnen inzetten."

In de Cyber Security Raad komen bedrijfsleven en terrorisme- en misdaadbestrijding bij elkaar. AIVD en MIVD opereren meer en meer samen. De politie krijgt te maken met jonge terroristen in spe. Ziet u privaat, overheid en inlichtingendiensten naar elkaar groeien?

"De Cyber Security Raad is een publiek-privaat samenwerkingsverband op strategisch-tactisch niveau. De laatste twee jaar is, mede door grote incidenten die publiek-private afstemming op hoog niveau vereisten,
een groeiend besef ontstaan van elkaars positie, werkwijze en de noodzaak tot nauwe samenwerking. Ook op operationeel niveau trouwens wordt kennis over cyberdreigingen en -incidenten uitgewisseld tussen private partijen onderling en ook met de overheid. Dat gebeurt binnen de wet, met mandaten en op basis van opgebouwd vertrouwen. Vertrouwen krijgen is een langzaam proces."

Wat zijn de grootste euvels op termijn?

"Afgelopen jaren gaf ik leiding aan een onderzoeksgroep over cyber security in Navo-verband. We kwamen tot de ontdekking dat we in cyber security twee niveaus node missen.
De ene is cyber securitywetenschap. We kennen zeer kundig onderzoek naar cryptografie, criminologie, sociale wetenschappen over beveiliging, specifieke technologie. Maar hoe past dat bij elkaar? Welke

combinatie van disciplines levert de beste cyber security op? Kun je dat wetenschappelijk onderbouwen en testen?
De volgende slag is cyber security engineering. Door instortende bruggen leerden we betere en veiligere bruggen te bouwen. Met cyber security zijn we lang zover nog niet. In de jaren zeventig dichten we al 150 gaten in onze Control Data systemen. Tot vandaag de dag gaan we steeds op dat praktische niveau aan de slag om dezelfde type gaten te dichten in steeds nieuwe systemen, bijvoorbeeld software in auto's. Maar hoe kom je nu tot structurele kennis en aanpak om de herhaling van dit soort fouten te voorkomen? Hoe kom je tot een veiligheidsfactor in het ontwerp en daarmee verder op het gebied van weerstand tegen online kwaadaardigheid?"

Terwijl we steeds afhankelijker worden?

"Ja, op mainframes waren er wachtwoordproblemen, met minicomputers nog meer en met pc's was het beheer weer een stuk moeilijker. Vandaag de dag kun je chips van auto's hacken. En van medische apparatuur, met veel ernstiger gevolgen. We leerden niet terwijl er steeds nieuwe computersystemen komen. Neem de smartphone, ook daarvan is de beveiliging niet eerst principieel goed opgezet.
Die cyclus weten we niet te doorbreken. Dat moet plaatsvinden in wetenschappelijk onderzoek en daarna in onderwijs op hoog niveau. Lessen moeten leiden tot theorie."

Dat klinkt dreigend.

"We moeten volwassen worden op dit niveau. Later dit jaar komt er een Navo-conferentie in Tallinn over dit onderwerp en ik probeer in Nederland ook een community van de grond te tillen om dit probleem van gebrekkige theorievorming aan te pakken.
Cyber security science als discipline is net in opkomst in Engeland, terwijl Defensie in Amerika die wetenschap ook wil vestigen in eigen land. Het is hard nodig, want nu is het met beveiliging dweilen met de kraan open."

Te zwak internet?

"Niet precies internet maar wel het feit dat we alles met alles koppelen zonder voldoende kritisch te zijn. Het woord 'Internet' gebruik ik niet zo snel, want er wordt snel gedacht aan World wide web. Ik kijk naar het brede cyber securityplaatje; dus ook naar 4G, RFID en NFC voor betalingen, medische systemen, auto's, smart grids en dergelijke. Beveiliging loopt ver achter, omdat we te weinig geleerd hebben van eerder falen en daaruit geen algemene conclusies trekken."

Er kwam voor Defensie 50 miljoen beschikbaar voor cyber operations. Een flink bedrag. Wat merkt u ervan?

"We werken er aan. Daar laat ik het even bij want een aantal collega's is met verschillende projecten bezig, zoals voor bescherming van Defensie. Reactief maar ook offensief. Dat liet de minister al weten en is dus openbaar."

Wat was de bijzonderste periode met internet?

"De periode vóór 1995, toen het publiek ging. Je zat er middenin maar we zagen werkelijk niet welke grote invloed het zou krijgen, anders waren we als pioniers misschien schatrijk geworden. Internet was een speeltje van wetenschap en onderzoek, een leuk protocolletje. Het was niet meer dan bijvoorbeeld Decnet dat we hier ook hadden.

Toen de eerste browser (Mosaic) kwam, was het snel kristalhelder welke mogelijkheden er in het verschiet lagen. Maar de eerste webpagina opbouwen vonden we toch nog een stuk moeilijker dan tekst opmaken met de line-editor die we zelf hadden gemaakt en het TNO tekstopmaakprogramma TOI voor rapporten."

Verwondering dat het web won?

"Ja, en zo snel. Ik heb toch het idee gekregen dat het web mensen de mogelijkheid bood om lekker te hobbyen, zelf pagina's te knutselen. In de eerste fase was het pionieren, maar het is zo enorm rijk geworden qua toepassingen. Van internetbankieren tot en met Facebook, steeds weer hele nieuwe vormen om bestaande functies online te brengen. Dat is fascinerend."

Gemak en plezier namen toe, het risico ook, maar daarvoor zijn de ogen gesloten en wordt Snowden nu gehypt?

"Precies, criminaliteit en spionage zijn er altijd geweest, maar nu het internetgebruik zo omvangrijk en alomvattend is geworden, zijn ook criminaliteit en spionage in alle geledingen doorgedrongen.
In 1977 was computercriminaliteit nieuw met ontvreemding van back-upmagneetbanden voor een losgeld van meer dan een miljoen gulden. Met een logische bom was de informatie in het computersysteem onklaar gemaakt. Dat was geheel nieuw en opzienbarend. Het eerste virus dateert van enkele jaren eerder. Nu hebben we dus al zo'n veertig jaar computercriminaliteit. De mensen zouden zich dus niet zo moeten verbazen bij weer een nieuwe cyberaanval of onthulling over cyberspionage."

Wanneer gaat internet plat en hebben we zo'n waarschuwing nodig?

"Er zullen delen uitvallen, want sommige knooppunten zijn zo attractief voor aanvallen en zo cruciaal dat ze een groter risico lopen. Daar zijn wel berekeningen over. Internet is opgezet voor redundantie, maar dat is niet genoeg. Het hoeft niet helemaal plat te gaan, maar bij uitval van enkele sleutelpunten kan de dienstverlening zo slecht worden omdat al het verkeer over B-wegen gaat.
Waarschijnlijk krijg je dan een deel dat lokaal nog wel werkt maar niet langer met de rest van de wereld."

Is telefonie over internet onveiliger dan vroeger via centrales, toen de telefoon het altijd deed?

"Vroeger was het ook kwetsbaar voor hackers. Zo stonden er ook allerlei tapinrichtingen op met achterdeurtjes die door vreemde mogendheden misbruikt zijn."

U doelt op de Israëlische tapinstallatie?

"Ik doel bijvoorbeeld op het afluisteren van zo'n honderd Griekse politici gedurende een jaar. In vier Ericsson AXE-eenheden was extra software geplaatst, waarbij mobiel telefonieverkeer ook een tweede weg inging en belandde op een vreemde plek."

Speelde dat in het begin van internet al? Heeft Vint Cerf het ooit over afluisteren gehad? Hij werkte immers voor Defensie?

"Beveiliging van de vertrouwelijkheid en integriteit, zo was het uitgangspunt, moet je altijd aan eindpunten van de verbindingen regelen en niet in het netwerk zelf. Dus met cryptografie. Dan heeft aftappen waar dan ook geen zin."

Bij de Radboud Universiteit zit een groep sterke hackers. Medestanders?

“Op heel veel terreinen. Maar er zijn er meer. Ook bij de TU Eindhoven waar ze de Javacard kraakten, zijn er dergelijke onderzoeksactiviteiten. Het kijken naar bijvoorbeeld de beveiliging van chips tot op bitniveau en evaluatie van producten volgens standaarden bij TNO is uitgemond in het bedrijf Brightsight. Hoeveel tijd heb je nodig om bij sleutelmateriaal in die chip te komen door die te etsen of met temperatuurwisselingen en elektromagnetische stimulatie te spelen? Buitengewoon boeiende wereld…”