# Nieuwe bedreigingen vragen om een nieuwe benadering

**Bernard Welten** is oud-politiechef en o.m. buitengewoon raadslid bij de Onderzoeksraad voor Veiligheid.

***Bernard Welten schetst een beeld van wat ons bedreigt op cybergebied. Te veel mensen reageren als de welbekende struisvogel, vindt hij, want de gevaren zijn reëel en zullen ongelooflijk veel impact hebben. Gelukkig biedt een crisis altijd ook kansen, maar het wordt wel tijd dat we die gaan pakken.***

Het is al weer bijna twintig jaar geleden dat ik met een ontvoeringszaak bezig was. Waar in voorgaande zaken het losgeld altijd op een bepaalde plek moest worden afgeleverd, werd nu geëist het over te maken op een bankrekening in een ver buitenland. Met de kennis van nu zal het u niet verbazen dat die rekening was geplunderd voordat wij erbij konden komen. Voor mij was dat toen de eerste kennismaking met een nieuw tijdperk dat zich steeds ontluisterender ontvouwt. Inmiddels ben ik al eens slachtoffer geworden van Ransomeware. Al mijn documenten versleuteld en na het betalen van losgeld kon ik de code krijgen.

## Onheilspellend

In het boek *Future Crimes* schetst een van 's werelds meest vooraanstaande veiligheidsexperts Marc Goodman een griezelig beeld van wat ons nog meer te wachten staat op het gebied van cybercrime. Niet alleen criminelen, maar ook bedrijven en zelfs landen maken gebruik van nieuwe zich ontwikkelende technologieën die ons buitengewoon kwetsbaar maken op manieren die we ons nauwelijks nog voor kunnen stellen.

Als we ons eerst tot de echte boeven beperken, Goodman beschrijft fenomenen als *the dark web*, de onheilspellende verzamelnaam voor sites die niet door Google geïndexeerd willen worden. Het is een marktplaats waar wapens, drugs en gestolen gebruikersdata verhandeld worden. Terwijl de massa surft op het reguliere web, loeren onder de oppervlakte cybercriminelen, hackers en phishers die miljoenen slachtoffers tegelijk maken met een gehaaide mail of die een DDOS-aanval voorbereiden.

> ***» Cybercriminaliteit kost ons tenminste 10 miljard per jaar, ca. 600 euro per burger***

De pakkans met die nieuwe vorm van criminaliteit is klein en de opbrengst groter dan activiteiten in de fysieke wereld. Sommige criminele organisaties zijn zo groot dat ze werken met een heus managementteam en een HR-afdeling om nieuw technisch talent te scouten. Resultaat? Denk aan de digitale bankroof in de VS in 2013, waarbij in tien uur tijd 36.000 transacties werden gedaan bij geldautomaten in 27 landen. Buit: 45 miljoen. Maar dat lijkt al bijna klein bier in vergelijking met de recente bekendmaking van cyberbeveiliger Kaspersky Lab dat een groepering van hackers in de afgelopen twee jaar circa een miljard dollar heeft buitgemaakt op circa 100 financiële instellingen wereldwijd.

## Bedreigingen

Men zegt dat de criminaliteit daalt. Dat is zeker zo als het gaat om de zichtbare vormen ervan. Maar ik ben er nog niet zo zeker van dat dit ook geldt voor de onzichtbare criminaliteit. Als banken niet vertellen dat ze zijn beroofd, is het op papier niet gebeurd.

Wat we wel weten: cybercriminaliteit kost de Nederlandse samenleving tenminste 10 miljard euro per jaar, aldus TNO. TNO baseert zich op Brits onderzoek. De resultaten zijn geschaald naar de situatie in Nederland. Die 10 miljard schade komt neer op 1,5 tot 2 procent van het bruto nationaal product, bijna 600 euro per burger in ons land.

Het aantal cyberincidenten verdrievoudigde in Nederland in 2014 ten opzichte van het jaar ervoor. Vijftig procent van alle aanvallen wordt volgens Fox-IT pas na maanden ontdekt. Hetzelfde bedrijf stelt dat het in 2014 gemiddeld 200 dagen duurde voordat een organisatie doorhad dat zij gehackt was.

Nederland heeft een van de grootste havens ter wereld en een van de beste luchthavens. Multinationals als Unilever, Shell, Philips, ASML hebben hun hoofdkantoren hier in Nederland. We zijn in Nederland grootgebruiker van mobiel internet en online diensten. Het lijkt niet te vermijden dat criminelen erin zullen slagen om organisaties binnen te dringen via het internet. Het plunderen van *the internet of things* is dankbaar werk voor de georganiseerde misdaad. Nieuwe doelwitten worden steeds vaker gezocht in controlesystemen die geïndustrialiseerde processen aansturen. Wat betekent dat voor defensie, voor de NS, voor waterleidingbedrijven, voor de financiële markt?

Dan zijn er nog de verhoudingen tussen landen. Tussen China en de VS is een bikkelharde cyberoorlog gaande waarvan niemand weet hoe ernstig de gevolgen wereldwijd kunnen zijn. Hillary Clinton heeft het over de Chinezen die 'alles hacken wat niet beweegt'. Jeb Bush pleit voor supersancties en rigoureuze cyberaanvallen als krachtig signaal. Men heeft het over een virtuele wapenstilstand. Oorlogstaal, zonder dat er een tank of een zelfs maar een drone aan te pas komt.

## Waar kennen we dit van?

Dit zijn reële dreigingen, maar te vaak denken mensen dat het wel mee zal vallen. We reageren niet of nauwelijks. Het lijkt op struisvogelpolitiek. Een gekoesterde bewustzijnsvernauwing. 'We kijken het nog even aan.' Ik noem het voorspelbare menselijke kortzichtigheid. Soms ook weten we ons niet echt raad met dreigingen en crises en vervallen we al snel in 'dat we het daadkrachtig moeten aanpakken'. Dat levert in de praktijk niet veel meer op dan meer van het zelfde. En het helpt ons niet.

Er zijn andere voorbeelden van maatschappelijke vraagstukken waar we niet meer wegkomen met dat soort reacties. Al in 2007 schreef Willem Middelkoop een glashelder boek: *Als de dollar valt.* Daarin beantwoordt hij honderd vragen over onze geldeconomie en de dreigende kredietcrisis. Centraal daarin is niet de vraag óf de dollar valt, maar wanneer en wat daarvan de gevolgen zijn. Door sommigen werd het als interessant betiteld, maar verder haalden velen de schouders op.

Begin 2015. Joris Luyendijk publiceert *Dit kan niet waar zijn*. Hij concludeert dat een crisis als in 2008 zo maar weer kan ontstaan. 'Structurele maatregelen om de burgers te beschermen tegen omvallende banken, zijn niet genomen,' stelt hij. 'Er is geen politieke discussie. Er is geen enkele partij die een duidelijke visie op de toekomst van de sector heeft. Ik heb het idee dat we nog niet eens in de bewustwordingsfase zitten.'

Miljarden moesten worden opgehoest om banken te redden. Er is niemand vervolgd en het lijkt weer *business as usual*. En wij denken nog steeds dat het wel overwaait. Zijn de diepere oorzaken van de crash van 2008 weggenomen, of is de financiële wereld nog altijd een tijdbom in het hart van onze samenleving?

Er zijn nog meer van die verhalen. Al Gore, *Een ongemakkelijke waarheid*. Een typisch verhaal van de gekookte kikker. De klimaatcrisis voltrekt zich zo rustig, dat we er aan gewend raken. Is het simpelweg gemakkelijker om de waarschuwingen te negeren?

> » *Overweeg serieus een instantie op te heffen als de doorbraak niet lukt*

## Oplossingen

Met cyberdreiging scheren we eveneens langs de rand van de afgrond. Het raakt direct aan onze veiligheid. Veel veiligheidsspecialisten zeggen dat het een keer heel goed mis moet gaan om de bewustwording te creëren. Een soort Pearl Harbor, of een 9/11. Maar dat is onzin. Want het gaat nu al regelmatig heel erg mis en net als bij de bankencrisis is er feitelijk maar bar weinig veranderd. Ook hier zeg ik met Luyendijk: dit kan niet waar zijn. Het kan niet waar zijn dat we het maar niet willen zien.

Is dit alles bangmakerij? Zeker, dat is ook de bedoeling. Maar ik ben een irrationele optimist. Uit dreiging en crises kan ook kracht ontstaan: in de mogelijkheid om bakens te verzetten. Om iets te gaan doen dat onder normale omstandigheden ondenkbaar zou zijn. De dreiging, de crisis bieden kansen.

Marc Goodman suggereert in *Future Crimes* ook oplossingen binnen de techniek. Digitale mieren die verdachte activiteiten in het netwerk signaleren en opruimen. Ik heb weleens een vergelijking met witte bloedlichamen in de maatschappij gemaakt. Net als in een lichaam zou de samenleving een soort immuunsysteem moeten ontwikkelen. Dat je op tijd ziet dat er wat mis is voordat het te laat is. Een soort maatschappelijke lymfen. Binnen de politie introduceerden we alweer tien jaar geleden het begrip de nodale oriëntatie. De virtuele slotgracht om te voorkomen dat via informatie, water, lucht en land narigheid binnen kan komen.

## Congestie en moestuintjes

Laten we eerlijk zijn. De politie kan dat niet allemaal bijbenen. Onlangs zei minister Van der Steur dat er meer technische rechercheurs aangesteld moeten worden, maar dat zijn druppels op een gloeiende plaat. Als het gaat om de bestrijding van criminaliteit wordt nog steeds te zeer uitgegaan van het strafrecht als hét middel. En het héé́ft een belangrijke functie, laat het vooral goed werken, maar het stamt ook uit de 19e eeuw. Als probleemoplosser heeft het zijn langste tijd gehad. Ik denk dat om twee redenen.

Politie en OM worden overvraagd en er treedt congestie op. Het systeem raakt vol. Het aantal mensen dat veroordeeld is, maar waarbij de straf niet, of nog niet, ten uitvoer wordt gelegd loopt letterlijk in de honderdduizenden.

Je ziet dat 'de markt dat ook aanvoelt', want wat wat 'the private justice' wordt genoemd, neemt hand over hand toe. Vormen van criminaliteit binnen het bedrijfsleven worden intern afgedaan. Daar komt dikwijls niemand meer van het OM aan te pas. De aangiftebereidheid is dramatisch laag. Er is een private bypass gemaakt die de strafrechtspleging links en rechts passeert. Ik denk dat we zouden schrikken van de hoeveelheid zaken als we dat getal zouden kennen.

De tweede reden waarom de traditionele repressie zijn


langste tijd heeft gehad, is het feit dat alle instanties die daarmee bezig zijn, veel te druk zijn geweest met zichzelf. Wij lijden aan een moestuintjescomplex. Eigen doelstelling eerst. Het is ongelooflijk weerbarstig om partijen zo met elkaar te laten samenwerken, dat de eigen targets ondergeschikt worden gemaakt aan het collectieve belang.

Nog steeds is het zo dat de linkerhand van de overheid vaak geen idee heeft wat de rechterhand doet. Het gebeurt met grote regelmaat dat iemand die veroordeeld is voor een strafbaar feit, wel gewoon een paspoort krijgt. In de Bijlmermeer kregen mensen een toeslag voor de opvang van een kind. Waarbij niet werd gecontroleerd of er eigenlijk wel een kind was. En zo zijn er heel veel voorbeelden. De politie zelf heeft nog steeds veel te veel de neiging achter de zoveelste boef aan te rennen die misbruik heeft gemaakt van het kwetsbare systeem.

Samengevat: de bestaande repressie loopt vast en de bestaande samenwerking maakt geen vuist. Kan het anders?

## Een nieuwe benadering

Ik bepleit graag een nieuwe oriëntatie op het denken over veiligheid, die beter past in het huidige tijdperk. Ik ben zelf betrokken geweest bij een aantal initiatieven die aan die nieuwe oriëntatie raken. Bij de top 600-aanpak in Amsterdam kwamen voor het eerst 34 partijen samen (zoveel kunnen er met één verdachte bezig zijn) om een einde te maken aan dat eindeloze ge-draaideur van criminelen.

Bij het initiatief 1 overheid proberen we de mogelijkheden dicht te schroeien dat iets weer kan gebeuren. Dan is het zaak niet te kijken naar het incident zelf en vervolgens iemand te vervolgen, maar vooral te kijken naar het patroon en de methodes, om dat te doorbreken: hoe gebeurt dit, hoe frequent, welke partijen zijn erbij betrokken?

Voorkomen is effectiever dan repressief handelen. Een voorbeeld: toen banken er achter kwamen dat pinautomaten geskimd werden, werd het patroon doorbroken door de pinautomaat te veranderen.

Ook voor de dreiging van cybercriminaliteit is iets dergelijks een realistisch perspectief. En dat nieuwe veiligheiddenken stoelt op twee pijlers:

1) doorbreek de scheiding van de aparte silo's die de veiligheidsinstanties nog steeds zijn
2) en geef nu eindelijk eens inhoud aan het begrip Publiek Private Samenwerking, dat ik inmiddels liever Privaat Publiek Partnership zou willen noemen.

## Gelijkwaardige samenwerking

Dat van die silo's is taai. De ambtelijke obstructie, de institutionele weerstand, de remmers in vaste dienst zijn fenomenaal. Dit is een traject van lange adem. Te veel mensen zijn van nature gewend om houvast te zoeken met bekende methoden. Te vaak horen we nog: "Dat kan niet, dat mag niet, we doen het al." Ook een aardige om horendol van te worden bij een geringe afwijking van het traditionele denken: "Dit brengt mijn minister in de problemen."

Mijn suggestie: als die doorbraak niet lukt, overweeg dan serieus om een instantie op te heffen en in een andere gedaante terug te laten komen.

Het tweede, inhoud geven aan PPS (PPP) is een enorme kans voor veiligheidsindustrie. En voor de overheid. Maar dat is nog niet echt doorgedrongen. De Nederlandse wetgeving kent geen expliciete grondslag voor PPS betreffende digitale veiligheid. Er zijn wat kaderregelingen. En daarom is er nu nauwelijks juridische ruimte om in PPS-verband te experimenteren en vernieuwende horizontale afspraken te maken. Daar moet veel meer werk van worden gemaakt. In de media, in de publicaties, in de politiek.

De wereld van de security is inmiddels net zo groot als de politie zelf. Het onderscheid tussen publiek en privaat is niet meer zwart-wit, maar het is een grijs gebied. Zoek naar concrete voorbeelden (die er echt al wel zijn) waar omheen samenwerking gestalte krijgt. Stem de doelstellingen met elkaar af, leen over en weer mensen uit. Zoek naar varianten waarbinnen informatie gedeeld kan worden. Begin, of ga door, niet aflatend. Werk op basis van gelijkwaardigheid. «