Als de *digitale* bom valt...

Vrijwel alle apparaten, fabrieken en infrastructuur worden aangestuurd door computers. Dat maakt cyberaanvallen een steeds interessantere manier van oorlog voeren. Hoe kwetsbaar is Nederland?

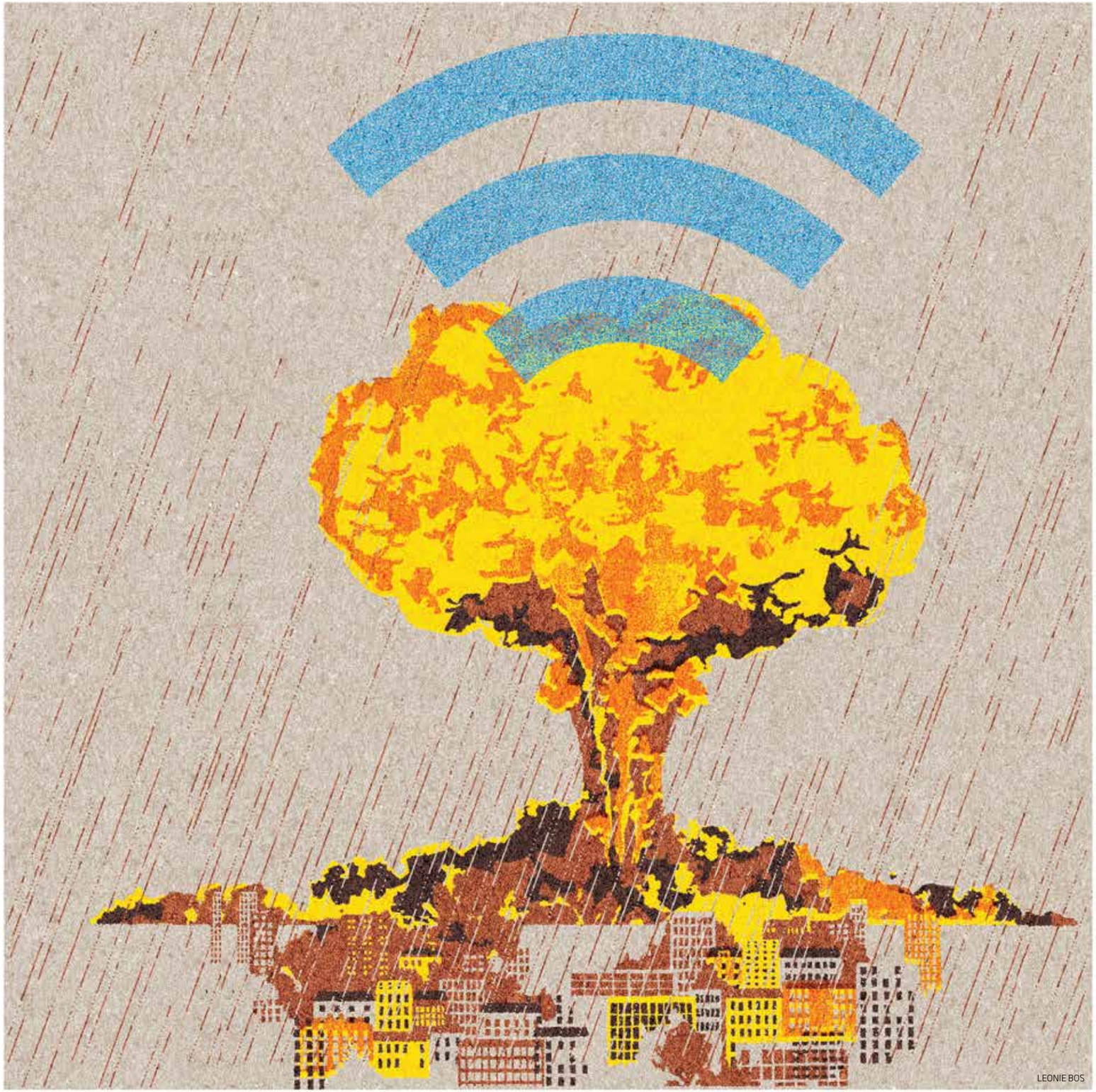
Door Ed Croonenberg

Om even over elf uur 's ochtends dreunt door de straten van Hoogvliet bij Rotterdam een zware explosie. Glas vliegt uit de sponningen, er klinkt gegil. Voordeuren zwaaien open, mensen rennen de straat op – sommige bloedend. Terwijl buren verbijsterd steun bij elkaar zoeken, rijst aan de heldere septemberlucht een zwarte wolk op. De bewoners weten genoeg: het gaat om Pernis, de ten noorden van Hoogvliet gelegen grootste olieraffinaderij van Europa.

Oudere bewoners herinneren zich dat het daar al eens eerder mis ging. Ook in 1968 vlogen na een grote ontploffing in Hoogvliet de glasscherven door de straten. Wonder boven wonder vielen er toen maar twee doden.

Terwijl de sirenes aanzwellen, klinkt een tweede klap. De rookwolk dijt uit en de lucht wordt zwaar van de stank. Veel ambulancebroeders dragen mondkapjes.

Op de eerstehulpposten van de Rotterdamse ziekenhuizen is de toestand chaotisch. Naast mensen met glaswonden worden ook slachtoffers binnengebracht met zware brandwonden en ernstige vergiftigingsverschijnselen. Het gerucht begint zich te verspreiden dat er veel doden te betreuren zijn. Terwijl de operatiekamers razendsnel in gereedheid worden gebracht, valt het licht uit. Een stroomstoring, juist op dit kritieke moment! Ogenblikken later starten de noodaggregaten op.



LEONIE BOS

'Tussen een Iraans besluit om zich te verdedigen en een ontploffing in Hoogvliet, zit nog een aantal stappen'


Hoe gemakkelijk kunnen cyberterroristen de industrie in ons land platleggen?
ANP

In Rotterdam breekt paniek uit. Mensen zien de hemel verduisteren, ademen de steeds giftigere lucht in maar tasten in het duister over wat er precies aan de hand is. Televisies werken niet meer, en ook het mobiele netwerk komt haperend tot stilstand. Als snel ontstaan rond de stad lange files van werknemers die het voor gezien houden en bewoners die het zekere voor het onzekere nemen. Eenmaal thuis of bij kennissen aangekomen blijkt dat ook op flinke afstand van de explosies de stroom- en telecomnetwerken niet meer functioneren.

Lange, chaotische uren later komt de informatievoorziening haperend op gang. In Pernis heeft een fatale samenloop van omstandigheden geleid tot de volledige verwoesting van een aantal benzine-reformeerinstallaties. Daarbij vielen tientallen doden. Onduidelijk is of er verband bestaat met de massale stroomstoring die kort daarop plaatsvond en die in grote delen van het land nog altijd voortduurt. In sommige ziekenhuizen hebben de noodstroomvoorzieningen het laten afweten. Bij een botsing tussen een diesellocomotief en een stilstaande intercity zijn vermoedelijk dodelijke slachtoffers gevallen.

Een aantal van de getroffen centrales komt pas na dagen weer op gang. Op het internet wordt het gerucht steeds sterker dat Nederland en zijn buurlanden zijn getroffen door een cyberaanval van nooit eerder geziene omvang. De beschuldigende vinger wijst al snel richting Iran. Dat land heeft een motief: de VS hebben enkele maanden eerder laten weten een gewapende aanval op Irans nucleaire installaties niet meer uit te sluiten. Na uitputtende debatten besloten een aantal Europese landen, waaronder Nederland, zich daarbij aan te sluiten. De Iraanse president Hassan Rouhani had daarop onheilspellend gedreigd terug te slaan 'op welk front dan ook'.

Cybersabotage

Hoe realistisch is dit scenario? Zijn hackers in staat complete industriële installaties op fatale wijze te ontregelen? Het antwoord is deels gelegen in de meest roemruchte cyberaanval tot nu toe: Stuxnet. Deze opmerkelijk geavanceerde computerworm werd in juni 2010 ontdekt. Het virtuele ondier besmette eerst Windows-computers, om daarna over te springen op zogenaamde Programmable Logic Controllers (PLC's) van het merk Siemens. PLC's zijn computers die industriële systemen aansturen. Ze worden geprogrammeerd met, in de meeste gevallen, Windows-pc's.

'Er zijn vele miljoenen PLC's op de wereld', zegt Eric Luiijf, die bij TNO de bescherming van vitale infrastructuren onderzoekt. 'Ze bedienen gaskleppen en pompen. Ze sturen wissels, slagbomen en seinen aan. Op Schiphol sturen ze de bagage-afhandeling aan, signaleren ze of er koffers klem zitten en zetten ze indien nodig de lopende band stop.'

Om iets stiekem stuk te maken, is het noodzakelijk tot in detail te weten hoe het in elkaar zit

Maar Stuxnet was niet ontworpen om bagageafhandelingen te ontwrichten. In plaats daarvan ging de worm op zoek naar PLC's die hogefrequentieregelaars aansturen. Dat is elektronica die wordt gebruikt om elektromotoren met extreme snelheden te laten draaien – snelheden die eigenlijk maar één toepassing kennen, namelijk het maken van nucleaire brandstof in een zogeheten ultracentrifuge.

Stuxnet sloeg toe in de Iraanse uranium-opwerkfabriek Natanz. Volgens cijfers van atoomwaakhond IAEA nam het aantal werkende Iraanse centrifuges in de zomer van 2010 flink af. Wat zich precies heeft afgespeeld blijft in nevelen gehuld, maar is wel voorstelbaar. Ultracentrifuges draaien op de grenzen van het fysiek haalbare. Als Stuxnet ze tot hogere snelheden heeft opgezweept, zullen de lagers het al snel begeven, met grote schade als gevolg. Omdat een opwerkingsfabriek duizenden centrifuges telt, zal de ramp niet meteen aan het licht zijn gekomen en kon de worm ongemerkt zijn verwoestende werk verrichten.

Toegegeven is het nooit, maar veel deskundigen nemen aan dat de cyberaanval onderdeel uitmaakte van Operation Olympic Games. Dat zou een geheime samenwerking met Israël betreffen om te voorkomen dat dat land bommenwerpers inzet tegen Iraanse nucleaire installaties. In *The New Yorker* werd Operation Olympic Games 'de eerste formele offensieve daad van pure cybersabotage door de VS tegen een ander land' genoemd.

James Bond

Als de VS samen met Israël een nucleaire fabriek kunnen ontwrichten, kunnen Iraniërs dan een Nederlandse raffinaderij opblazen? 'Tussen een eventueel Iraans besluit om zich te verdedigen en een ontploffing in Hoogvliet, zit nog een aantal stappen', zegt Bart Jacobs, hoogleraar digitale veiligheid aan de Radboud Universiteit in Nijmegen. 'Dat is niet zo eenvoudig zonder gedetailleerde kennis van hoe de procesindustrie zaken geregeld heeft. Het kan echter wel.'

Om iets op een stiekeme manier stuk te maken, is het dus noodzakelijk tot in detail te weten hoe het in elkaar zit. Dat geeft cybersabotage van een tamelijk hoog *James Bond*-gehalte. Volgens een intrigerende reconstructie die in juni vorig jaar in de *The New York Times* verscheen, hadden Israëlische spionnen zich een duidelijk beeld gevormd van het soort ap-


De Iraanse president Mahmoud Ahmadinejad inspecteert de uranium-opwerkfabriek in Natanz. De fabriek kreeg te maken met een gerichte cyberaanval.
IRANIAN PRESIDENT'S OFFICE

'Nederland kraakt onder cyberaanvallen'

TNO-onderzoeker Eric Luiijf schrijft voor de Rijksoverheid scenario's om het cyberrisico voor Nederland te kunnen inschatten. In het rapport *Scenario's Nationale Risicobeoordeling* uit 2010 beschrijft hij hoe de deelname van Nederland aan ingrijpen in de denkbeeldige staat Conflictistan leidt tot een spervuur van relatief beperkte aanvallen die niettemin bij elkaar het leven van gewone Nederlanders dagenlang ontregelen.

De aanval begint 's ochtends met het verstoren van de verbindingen van de Nederlandse troepen in Conflictistan, gevolgd door het uitvallen van interne servers van de overheid en de Tweede Kamer. Ambtenaren verlaten de ministeries omdat ze niet meer bij telefoonnummers, agenda's en dossiers kunnen en omdat het mailverkeer plat ligt. Tegen het middaguur vallen de bagagesorteersystemen van Schiphol uit. Ondertussen laat een softwareworm smartphones massaal naar 112 bellen, dat daardoor onbereikbaar wordt. Vertrouwelijke militaire documenten verschijnen op WikiLeaks. In Gelderland valt de stroom uit. De website van *De Telegraaf* kopt: 'Nederland kraakt onder cyberaanvallen, wat nu?'

De dagen erna wordt de AEX gehackt, maken wormaanvallen de privé-gegevens van bankcliënten onbereikbaar en vinden er diepe hacks plaats in de systemen van grote gemeenten. Het vertrouwen van burgers in de overheid verdampt. Voor de pinautomaten die nog werken verschijnen lange rijen.

Het is een worst-case-scenario, maar volgens Luiijf zeker niet ondenkbaar. 'Alle activiteiten beschreven in het scenario zijn technisch gezien mogelijk en zijn ieder afzonderlijk al eens ergens op de wereld voorgekomen. Het wordt daarom voorstelbaar geacht dat dit scenario zich in de komende vijf jaar kan voordoen.'

Het rapport is te downloaden via **goo.gl/HwKXCh**

In 2005 wisten hackers door te dringen in Braziliaanse energienetwerk, waardoor bij 17 miljoen mensen het licht uit ging.
FLICKR/FERNANDO STANKUNS

paratuur dat in Natanz stond te draaien. De centrifuges waren gebaseerd op een ontwerp van Abdul Khadir Khan, de Pakistaanse kerngeleerde die zijn gevaarlijke kennis bij het Nederlandse Urenco opdeed. Het toeval wilde dat Moammer Khadaffi ooit nucleaire ambities had en over dergelijke centrifuges beschikte. Toen de wispelturige dictator in 2003 weer bij het Westen in het gevlij trachtte te komen, droeg hij de centrifuges over aan de Amerikanen, die ze ergens in Tennessee opsloegen.

Op basis van de Israëlische informatie bouwden de Amerikanen met de Libische centrifuges een stukje Natanz na om de ongebruikelijk complexe softwareworm zo realistisch mogelijk te testen.

Onder de grootste mogelijke geheimhouding werd de worm verfijnd tot er daadwerkelijk centrifuges onder luid geraas de geest gaven. Stuxnet was ongetwijfeld niet alleen de slimste, maar ook de duurste worm ooit.

Het vergde eveneens precisiewerk om Stuxnet ter plaatse te krijgen. Zulke geheime malware zomaar het internet op slingeren, was geen optie. Israëlische spionnen zouden ervoor moeten zorgen dat een medewerker van de fabriek de worm via een USB-stick het netwerk op zou laten. ‘Uiteindelijk is er altijd wel een idioot te vinden die niet nadenkt over dat ding in zijn hand,’ zegt een anonieme bron in het artikel van *The New York Times*

> Een alarmerend probleem is de levendige handel in softwaredefecten aan geheime diensten

– het artikel is noodzakelijkerwijs geheel op anonieme bronnen gebaseerd.

Hoe knap ook, Stuxnet richtte zich binnen de opwerkingsfabriek maar op één systeem waarvan de inlichtingendiensten toevallig alle technische details kenden. Dat veroorzaakte schade, maar schakelde niet de hele fabriek uit. Om een catastrofe te veroorzaken, moeten heel veel afzonderlijke sabotagestappen worden gecombineerd. En dat is heel moeilijk. ‘Je kunt misschien zorgen dat de benzine een verkeerde samenstelling krijgt’, zegt Luiijf. ‘Een enorme vlam uit de affakkelpijp kan ik mij ook nog voorstellen, maar een allesvernietigende explosie lijkt mij niet realistisch.’ Het in serie platleggen van energiecentrales lijkt hem buitengewoon lastig omdat die volgens hem allemaal redelijk uniek zijn. Luiijf: ‘Ook al kun je in de PLC komen, dan nog moet je wel precies weten wat er achter output X of Y zit. Zulke kennis over het systeem is essentieel.’

Dat betekent niet dat we rustig kunnen gaan slapen. Op 1 januari 2005 wisten hackers door te dringen in de besturingsconsoles van het Braziliaanse energienetwerk, waardoor bij 17 miljoen mensen het licht uit ging.

‘Enkele jaren geleden waren hackers één commando verwijderd van het stilleggen van de stroomvoorziening in een groot Europees land’, zegt Luiijf. ‘Netwerken van met name nutsbedrijven worden dagelijks afgetast om te kijken of je er binnen kunt komen.’

De anonieme, mogelijk staat-gelieerde dreiging die hier achter zit, wordt in de security-wereld aangeduid als advanced persistent threat. Zodra een systeem wordt gekraakt, kunnen er rare dingen gebeuren.

‘Stel’, zegt Bart Jacobs, ‘er komt op kabinetsniveau een anonieme dreiging binnen: als Nederland niet voor of tegen die en die resolutie in de Veiligheidsraad stemt, dan worden van een afstand de sluizen opengezet. Hoe moet je daar als kabinet mee omgaan? Het enige wat je echt kunt doen is ervoor zorgen dat je eigen systemen op orde zijn. Daar wordt nu aan gewerkt, met name in de vitale infrastructuur. Ik durf en wil geen uitspraak te doen over hoe we ervoor staan.’

Hartbewaking

Wanneer is een systeem ‘op orde’? Het is tot nu toe onmogelijk gebleken complexe software te maken waar zich geen zwakke plekken of regelrechte fouten in bevinden. Een alarmerend probleem is dat kennis over die zwakke plekken handelswaar is geworden. ‘We zien een levendige bedrijvigheid van mensen die softwaredefecten vinden en die verkopen aan nationale geheime diensten’, zegt programmeur en natuurkundige Wietse Venema, verbonden aan het T.J. Watson Research Center van IBM.

Bedrijven als Microsoft waren altijd bereid flink te betalen voor door derden opgespoorde fouten in hun software. Helaas bieden geheime diensten tegenwoordig meer. Dat past in de bredere trend dat gegevens van allerlei aard, gevonden of gestolen, op het internet aan de hoogste bieder worden verkocht.

Dat is potentieel erg gevaarlijk voor systemen die veel minder uniek zijn dan elektriciteitscentrales. De Amerikaanse Food and Drug Adminstration (FDA) gaf afgelopen juni een waarschuwing uit over cyberveiligheid van medische apparatuur. ‘Als je weet dat pacemakers tegenwoordig worden bijgeregeld via WiFi, begrijp je hoe gevaarlijk dat in feite is’, zegt Luiijf. ‘In Nederland is dit jaar hartbewakingsapparatuur aangetroffen die muziek stond te delen via het programma Kazaa. Ik raad ook aan eens te googelen op *hack insuline pump*.’ Wie dat doet, staat al snel versteld van het gemak waarmee de besturing van insulinepompen is over te nemen.

De grote paradox is dat de computerisering van de apparaten om ons heen voortdendert, terwijl cybercriminaliteit, zowel door overheden als bendes, steeds professioneler wordt. Dat maakt ons kwetsbaar. ‘In een moderne auto zitten zo’n 120 microprocessoren’, zegt Luiijf. ‘Ik maak mij dan ook zorgen over de monteur die ’s avonds op internet porno zit te kijken of illegale software downloadt en de volgende ochtend dezelfde laptop aan mijn auto vastkoppelt.’ De mensen die niet stilstaan bij het besmettingsgevaar dat ze zelf vormen, zijn de zwakste schakel. ■

> ‘In Nederland is dit jaar hartbewakingsapparatuur aangetroffen die muziek stond te delen via het programma Kazaa’

Bart Jacobs, hoogleraar digitale veiligheid aan de Radboud Universiteit in Nijmegen.
RADBOUD UNIVERSITEIT

Meer informatie

Misha Glenny schreef diverse boeken over de internationale cybermisdaad waaronder *Bodley Head* (2011)

Dark Market beschrijft de levendige handel in gestolen gegevens en hacktechnieken in *Cyberthieves, Cybercops and You* (2011)

Lees de reconstructie van de **Stuxnet-aanval** op Iran van *The New York Times* op **goo.gl/AsGRj**