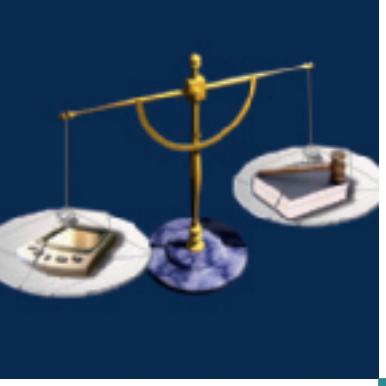

COLUMN

Kritische infrastructuur kritisch bekeken?

Column **Nico van Eijk**

Vliegtuigen storten nooit 'zomaar' neer. Bij het ontwerpen ervan gelden strenge eisen die de veiligheid moeten waarborgen. Een belangrijke voorwaarde is dat het uitvallen van één enkel onderdeel nooit fatale gevolgen mag hebben.Kritische systemen worden daarom dubbel uitgevoerd. Dit principe wordt ook wel 'redundancy' genoemd.

In het verleden golden vergelijkbare uitgangspunten ten aanzien van de communicatie-infrastructuur. Het beste voorbeeld is het klassieke telefoonnetwerk dat ook bleef werken wanneer de stroom uitviel: het had namelijk een eigen stroomvoorziening. Ook voor kabeltelevisienetwerken waren er technische voorschriften die er mede op gericht waren om de kwaliteit en continuïteit te garanderen. Gaandeweg zijn dergelijke ontwerpeisen verdwenen: ze werden gezien als onnodige regulering en de markt zou haar werk wel doen.

Er was wat aandacht voor de problematiek toen de millenniumkoorts uitbrak en gevreesd werd dat vanwege falende computers op 1 januari 2000 een algehele chaos zou uitbreken. Onderzoek wees uit dat bijvoorbeeld mobiele netwerken op grote schaal zouden uitvallen wanneer de stroomvoorziening zou stokken. Er zijn sindsdien enige acties ondernomen om ervoor te zorgen dat in tijden van nood ten minste een basaal niveau van communicatie overeind blijft, de zogenaamde NoodCommunicatieVoorziening (NCV).

Dit neemt niet weg dat in een tijdperk waarin elektronische communicatie steeds belangrijker wordt het uitvallen van netwerken alleen maar lijkt toe te nemen. Software upgrades gaan fout, als gevolg waarvan mobiele netten uitvallen of essentiële diensten niet meer functioneren (zoals bij het laatste Blackberry-incident). Met regelmaat zijn er storingen bij voice over ip-aanbieders waardoor hun klanten in delen van het land niet meer kunnen bellen. Zendmasten raken in brand en storten in. En ook de veiligheid van internettransacties raakt gecompromitteerd (zie de Diginotaraffaire).

Dit is een goed moment om meer aandacht te besteden aan kritische infrastructuren. Daarmee doel ik op voorzieningen die van cruciaal belang worden geacht voor het functioneren van de samenleving. Denk aan wegen, water, gas, licht, maar ook communicatie. Kwaliteit en continuïteit moeten gewaarborgd zijn, ongeacht of er concurrentie bestaat of niet. De schade die door falen optreedt, is daarvoor te groot.

De nieuwe telecommunicatiewet, waar de Eerste Kamer nog mee moet instemmen, biedt gelukkig een kapstok. Aanbieders van communicatienetwerken kunnen voortaan worden verplicht om passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en integriteit van hun netwerken en diensten te beheersen. Voor wat spraaktelefonie betreft, zijn de regels nog preciezer: alle noodzakelijke maatregelen moeten worden genomen om de beschikbaarheid zo volledig mogelijk te waarborgen in geval van een technische storing of uitval van het elektriciteitsnetwerk. Nadere regels kunnen worden gesteld en verplichtingen kunnen worden opgelegd. Daartoe behoort ook het laten uitvoeren van een veiligheidscontrole door een onafhankelijke deskundige. Bovendien komt er een meldplicht voor storingen en integriteitsinbreuken.

Verdere uitwerking vindt momenteel plaats via een ministerieel conceptbesluit waarover de markt is geconsulteerd. Dit besluit is echter nogal rudimentair en gaat vooral over een continuïteitsplan dat moet worden opgesteld door de aanbieders. Voor spraaktelefonie wordt nog geregeld dat aanbieders dienstverleningsovereenkomsten met relevante leveranciers en servicediensten moeten afsluiten om problemen met veiligheid en integriteit zo snel mogelijk te verhelpen. De vraag is of hiermee belangrijke risico's zijn afgedekt. Nieuwe incidenten zullen waarschijnlijk tot aanscherping leiden.

De extra kosten voor continuïteitsvoorzieningen zullen de aanbieders wel weer doorberekenen aan de gebruikers. Maar dat doen de luchtvaartmaatschappijen ook.