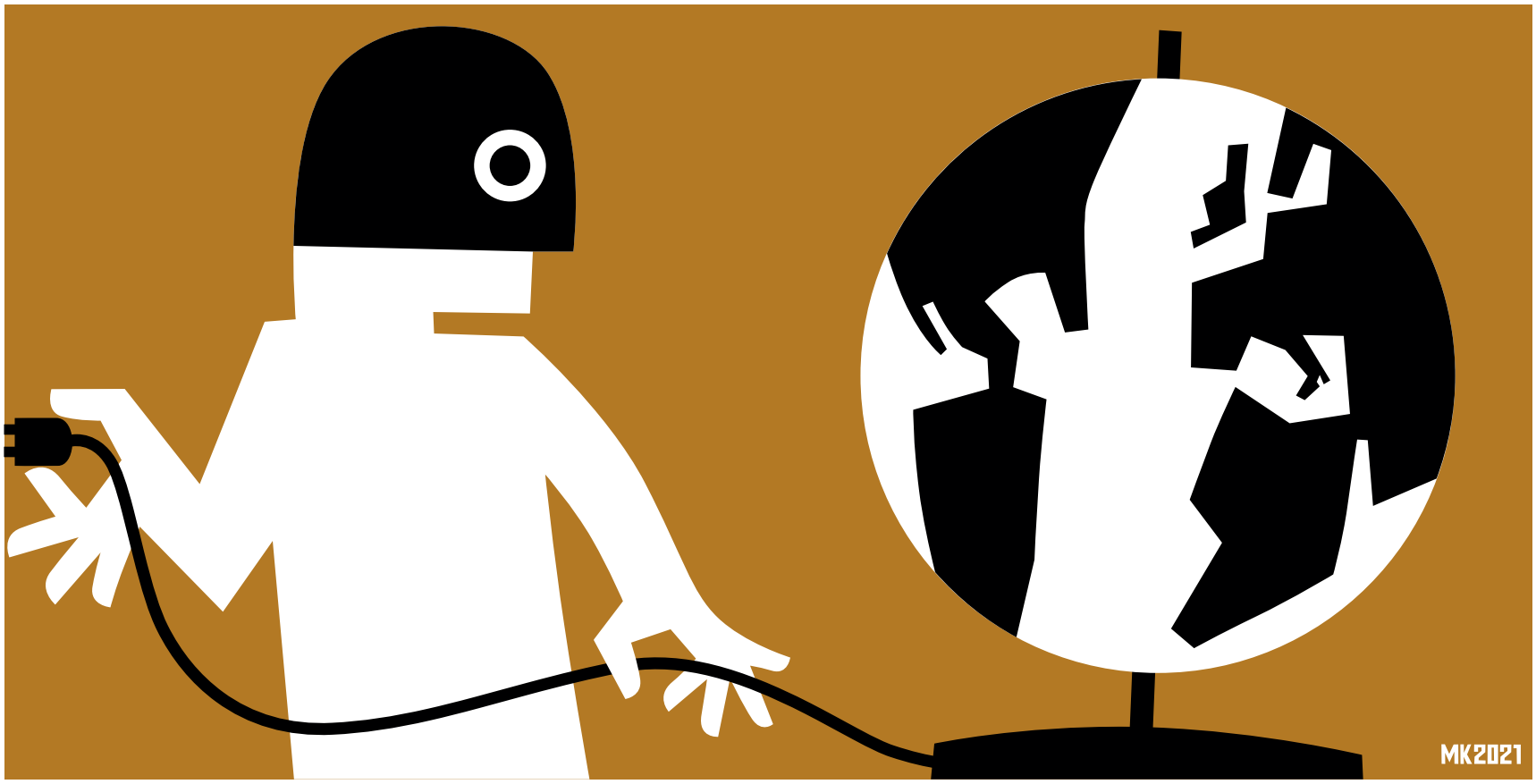

ILLUSTRATIE: MAX KISMAN VOOR HET FINANCIEELE DAGBLAD

ENERGIE

Voorzieningszekerheid wordt steeds meer virtueel

Met stijgende verbazing volg ik de perikelen rond het stilleggen door een aanval met gijzelsoftware van de Amerikaanse *Colonial Pipeline*. De gijzeling van de pijplijnsystemen met ransomware van de hackergroep DarkSide bracht deze nieuwe vorm van risico's voor de voorzieningszekerheid nog weer eens scherp voor het voetlicht.

De afhankelijkheid van de hele oostkust van de Verenigde Staten van dit pijpleidingsysteem voor olieproducten als benzine, kerosine en diesel was alom bekend bij mensen die zijn ingevoerd in het Amerikaanse energiesysteem. Het pijpleidingsysteem loopt van het raffinagecentrum in Houston tot aan New York en levert dagelijks ongeveer 2,5 miljoen vaten aan genoemde olieproducten.

Noordelijker gelegen steden aan de oostkust worden zelfs deels over de weg bevoorraad, wat bij sneeuw en ijzel al een paar keer voor leveringsproblemen heeft gezorgd. Nu werden consumenten getroffen van Texas tot aan New York. De rijen bij de benzinestations waren beelden die de meesten zullen associëren met de oliecrisis van 1973. Nu staan er rijen aan de pomp door gijzelsoftware van cybercriminelen, zo luidt het eerste oordeel, en waarschijnlijk niet door een geopolitiek conflict.

GEOPOLITIEK

Menige studie op het gebied van energie met daarin een paragraaf over voorzieningszekerheid haalt nog steeds de oliecrisis van 1973 aan als het beste voorbeeld van het risico op het onderbreken van de energievoorziening. Een dergelijke ouderwetse geopolitieke storing in de levering van energie komt echter veel minder vaak voor dan allerlei ander falen. Toch kunnen ook cyberaanvallen herleid worden tot kwaadwillenden van statelijke aard en met dit nieuwe wapen doelgericht de energievoorziening — en andere publieke diensten — ontregelen in een bepaalde sector en/of land.

Cyberaanvallen kunnen naast door aan staten gelieerde groepen ook worden verricht door op geld beluste lieden, door nieuwsgierige of ideologisch gedreven eenlingen of een combinatie van voorgenoemde. Een succesvolle aanval op een van onze energiesystemen is ons land tot dusver bespaard gebleven. Het is de vraag of dit het gevolg is van toeval, of van het op orde hebben van de Nederlandse verdediging.

Cybersecurity rond energievoorziening behoeft de volle aandacht

- Toename van zon- en windenergie leidt tot meer smartsystemen zoals slimme meters
- Intensieve uitwisseling van data introduceert nieuwe kwetsbaarheden

SUMMIER

In vergelijking tot het doorwrocht beleidsdocument van het Amerikaanse cybersecurity- en infrastructuuragentschap (Cisa), is de publieke informatie die de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum delen over bescherming van vitale infrastructuur nogal summier. Wellicht willen ze de kat niet op het spek binden, maar de VS laten zien dat iets meer informatie toegankelijk maken voor een breed publiek best kan zonder vitale gegevens prijs te geven.

Afgezien van de regelmatige crisisoefeningen in Nederland, en wetgeving die voorschrijft dat verschillende energiebedrijven op grond van hun zorgplicht adequate maatregelen moeten nemen, zou ook een rapportage over de staat van het uitvoeren van deze adequate maatregelen de informatievoorziening niet ontsieren.

Eerdere voorbeelden van het falen van vitale infrastructuur hebben ertoe geleid dat zowel de Verenigde Staten als ook de Europese Unie dit in de afgelopen jaren veel hoger op de veiligheidsagenda hebben geplaatst. Mocht vitale infrastructuur, zoals onze energievoorziening, onverhoopt toch stilvallen, dan zijn de rijen die we voor Amerikaanse benzinepompen zagen maar één voorbeeld van de mogelijke gevolgen.

Wat te denken als een kwaadaardige hacker succesvol het elektriciteitsnet weet te infiltreren. Dan vallen niet enkel de computer en betaalsystemen in benzinepompen uit, maar ook andere van stroom afhankelijke processen in onze maatschappij. De weerbaarheid van bijvoorbeeld steden bij een toenemende verknoping en digitalisering van het energiesysteem verdienen hierbij ook speciale aandacht.

Waar criminelen steeds ingenieuzer worden, worden energiesystemen in Europa steeds complexer. De energietransitie vraagt dat verschillende energiesystemen steeds vaker 'smart' en geïntegreerd zijn, om zo steeds meer veranderlijke energieproductie uit zon en wind te kunnen inpassen. Het vraagt slimme meters en slimme apparatuur met een intensieve data-uitwisseling via online netwerken. Dit introduceert nieuwe kwetsbaarheden.

Vorig jaar nog maakte de Europese koepelorganisatie voor transmissienetbeheerders van elektriciteit Entso-E bekend dat het bewijs had voor een succesvolle cyberinfiltratie. Alhoewel de actie beperkt leek tot de kantoornetwerken zijn de precieze details, net als bij de Colonial-pijpleiding, nog onbekend. Zonder nadere informatie ontstaat het idee dat een succesvolle aanval op het Europese energiesysteem eerder waarschijnlijk wordt dan andersom.

AFHANKELIJKHEID

De talrijke publiek bekende infiltraties op energienetwerken laten zien dat de recente gijzeling niet op zichzelf staat, noch dat deze beperkt is tot de VS, oliepijpleidingen of een bepaald type kwaadwillende. De verstoring toont bovenal onze afhankelijkheid van steeds verder gedigitaliseerde energiesystemen.

Het bevestigt dat in voorzieningszekerheidsanalyses ook cybersecurity de volle aandacht behoeft, zowel van onze overheidsdiensten als van de verschillende bedrijven die in Nederland zijn belast met de plicht adequate maatregelen te nemen.

Energiebedrijven moeten 'adequate maatregelen' nemen, maar de rapportage daarover is summier

Coby van der Linde is directeur Clingendael International Energy Programme (CIEP). Reageer via opinie@fd.nl.