DE KEUS VAN INGENIEUR TEUS

ir. Teus van der Plaat

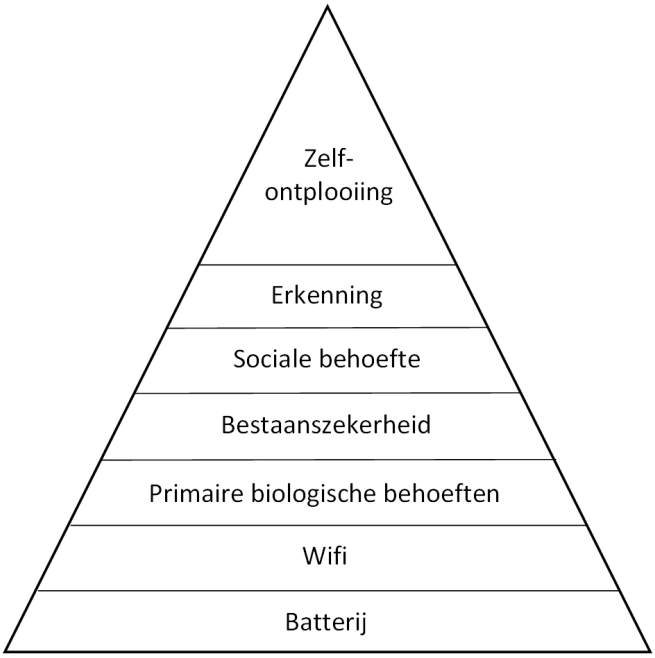
RESILIENCE
OPERATIONELE NOODZAAK

Op dringend verzoek van de hoofdredacteur geef ik in deze column mijn alternatieve analyse van de noodzakelijke resilience in de it van defensie. De uitspraak dat 'als alles stilvalt defensie doorgaat' hint op de aanwezigheid van de nodige resilience. Het is een thema dat zeer actueel is. Aangezien ik geen kennis heb van hetgeen zich op dit vlak in GRIT afspeelt is dit mijn analyse vanuit mijn gezonde verstand. Ik zal me wel moeten beperken tot een paar voorbeelden van dit fenomeen in het algemeen en verbindingen in het bijzonder want uitputtend behandelen valt volledig buiten de scope van een column.

Definitie resilience

Allereerst heb ik in de literatuur nagezocht wat er exact bedoeld wordt met de term resilience. Er komen verschillende vertalingen tevoorschijn, zoals veerkracht, incasseringsvermogen, het vermogen een oorspronkelijke vorm terug te krijgen, herstellingsvermogen, etc... kortom heel veel gezichtshoeken.

Bij de huidige defensie ict-organisatie gaat het uiteraard vooral om dingen als cyber resilience, data resilience, personele en organisatorische resilience, uitwijk en nog veel meer. In dit kader wil ik een paar deelaspecten bespreken, de power, operating system en de datacenter resilience.



Power resilience

Als we van een afstand naar de ict-operaties van defensie kijken is het eerste wat aanwezig moet zijn de stroomvoorziening. Diverse militairen met veel ervaring in recente operaties hebben mij verzekerd dat voor hun GEEN POWER, GEEN OPERATIE betekent. De stroomvoorziening is cruciaal, of dat nu het gewone vredeselektriciteitsnet is of voldoende batterij power en aggregaten voor mobiele operaties.
Immers, zonder stroom werkt er geen enkele computer, verbinding, radionetwerk en in toenemende mate ook geen enkel wapen.

De voormalige projectleider van Purple Nectar verzekerde mij dat voor een militair in de bekende piramide van Maslow de onderste laag power is. Zonder stroom begin je tegenwoordig helemaal niks. In zowel de statische, deployed en mobile operaties dient de stroomvoorziening resilient aanwezig te zijn.

Aangezien defensie zeker in het statische domein zeer veel gebruik maakt van commerciële voorzieningen (bijvoorbeeld de smartphone van elke defensiemedewerker) is de eerste vraag die dan opkomt of deze voorzieningen, waar we dus zeer van afhankelijk zijn, voldoende resilient zijn. Hoe vaak hoor je niet mensen zeggen die niet bereikbaar waren: “Mijn batterij was leeg”. Om een aspect er specifiek uit te pikken, de vier mobiele netwerken van Nederland hebben een batterij backup van ca. 20 minuten tot maximaal 1 uur. C2000 moet volgens de specificaties een batterij backup hebben van 8 uur. Aangezien er tegenwoordig ongeveer niks meer werkt zonder deze voorzieningen en defensie niet zelf over een dergelijk landelijk dekkend mobiel netwerk beschikt hebben we hier denk ik de eerste gevoelige resilience case te pakken.

Het NAFIN heeft overigens wel de nodige voorzieningen op dit vlak, maar dat is een vast netwerk, en heeft (nog) geen mobiele uitlopers conform de 3GPP standaards. Daarnaast komt het maar op een beperkt aantal plaatsen en beslist niet op elke vierkante kilometer van Nederland.

Als nu in grote delen Nederland werkelijk eens een flinke stroomstoring optreed dan is ‘Leiden en ik denk ook defensie in last’. Internet doet het niet meer, de mobiele netwerken liggen er binnen de kortste tijd uit, kortom het wordt een grote puinhoop. Mogelijk draaien de datacenters dan door, maar als de rest van de (mobiele) communicatievoorzieningen eruit ligt vanwege stroomstoringen heb je daar verder ook weinig aan. De vraag is wat dan de uitspraak ‘als alles stilvalt defensie doorgaat’ nog voor inhoud gegeven kan worden.

Hoe kunnen we dit eerste resilience probleem waar ik in mijn analyse tegen opliep relatief eenvoudig oplossen op een innovatieve manier? De eerste reactie is UPS systemen van voldoende capaciteit installeren bij het backbone netwerk van de mobiele operators en bij de basisstations in Nederland. Die laatste zijn er ongeveer tussen de 3500 en 5000 per operator dus je praat dan over alleen al 15.000 tot 20.000 opstelpunten, inclusief C2000. Hoe krijg je daar backup power geïnstalleerd die het een paar dagen tot een week uithoudt? Dit wordt een zeer kostbare operatie. Ik schets een alternatieve oplossing voor het power probleem.

De elektrische auto als oplossing voor het power probleem!

Privé heb ik een elektrische auto besteld van een Duitse crowdfunding startup uit München genaamd Sono Motors (bestelnr 7209!). Zij brengen een zeer interessante CO2 neutrale innovatieve en goedkope auto uit genaamd de SION (20.000 euro), die niet alleen elektrisch kan worden opgeladen, maar hij kan ook 2-fase en 3-fase stroom leveren uit zijn accu. De accu heeft een capaciteit van 35 tot 45 KWh waarmee je minimaal 250 km kan rijden, maar waarmee

ik mijn privé huishouden ook bijna een week van stroom kan voorzien. Een gemiddelde moderne energiezuinige macro mobiele cel of netwerkknooppunt heeft een stroomafname van een paar honderd watt. Dat betekent dat je uit zo'n auto accu dagenlang een mobiele mast van stroom kan voorzien. Er zijn ook andere EV auto's waar dit mee kan; ik kies echter deze omdat hij zo goedkoop en innovatief is!

Mijn innovatieve voorstel is om alle 50.000 defensiemedewerkers, militair en burger, voor hun vervoer en op vrijwillige basis te voorzien van zo'n auto. Ik schat in dat een flink deel van de populatie mee zou doen onder de defensievoorwaarden. Deelname hangt uiteraard sterk af van de verdeling van de financiering, die nader onderzocht moet worden. Bij een massale stroomuitval in Nederland moeten ze beschikbaar zijn om, via een slim toewijzingssysteem, naar de dichtstbij gelegen bestemming te rijden met de auto en met hun 3-fase stekker stroom gaan leveren aan onder andere de mobiele basisstations. Dit moet dan gebeuren, als het kan, binnen de termijn waar de bestaande batterij backup de power kan garanderen (Dus binnen ca 20 minuten tot 1 uur).
Ook andere belangrijke datacenters en netwerkknooppunten, voor zover niet reeds voorzien van noodstroom, worden op deze wijze zeer snel voorzien van backup stroom. Bij grote complexen moeten meer auto's parallel gaan staan om voldoende capaciteit te leveren.

De overheid/defensie moet de mobiele en netwerkoperators de verplichting op kunnen leggen een aansluiting en parkeerplaats(en) te maken waarop de auto's makkelijk kunnen aankoppelen en binnen korte tijd zijn alle Nederlandse opstelpunten, netwerkknooppunten etc, die getroffen zijn door de stroomuitval, potentieel voorzien van een batterij backup van bijna een week. Overigens kunnen deze punten tegelijk ook dienen als laadpalen voor auto's als de power wel aanwezig is. Het bijzondere aan de auto is dat hij ook zonnecellen in de carrosserie heeft geïntegreerd en hij kan tot ca. 30 km per dag of 1200 watt piek opladen met de zonnecellen die in de carrosserie zijn verwerkt. Verder is dan elke deelnemende medewerker verplicht om zijn batterij altijd zo goed mogelijk opgeladen te houden. Uiteraard mogen de defensiemedewerkers privé ook in deze auto's rijden en wordt voor hen de woon-werk vergoeding afgeschaft. Op defensieterreinen worden massaal laadpunten gemaakt voor bidirectionele voeding en lading. Aan de slogan 'als alles stilvalt kijkt men naar defensie' kan dan voor wat betreft stroomvoorziening op een innovatieve manier inhoud gegeven worden.

Het voordeel van deze voorziening is dat met een investering van een paar honderd miljoen euro in een klap het power probleem voor vitale voorzieningen is opgelost en alle deelnemers een mooie milieuvriendelijke CO2-uitstootbeperkende secundaire arbeidsvoorwaarde hebben! Hier staat uiteraard tegenover dat ze altijd bereid moeten zijn onmiddelijk in actie te komen bij voorkomende stroomstoringen en zelf de oplaadstroom moeten betalen om de accu op peil te houden. Door aanschaf van privé zonnepanelen zijn deze kosten echter tot een zeer gering bedrag te minimaliseren.

Datacenter resilience

Voor iedere organisatie en de krijgsmacht in het bijzonder is het datacenter cruciaal voor het leveren van diensten aan de organisatie. Uitval van een compleet datacenter is een ramp, mits er een goede uitwijk is die weer snel operationeel kan komen. In de oude defensie constellatie is sprake van twee datacenters en een uitwijk. Gezien de opgelopen militaire

spanningen in de wereld en het dreigingsbeeld, kan ik mij voorstellen dat dit een ongewenste en veel te kwetsbare situatie is. Immers, hoe goed de centra zelf ook beveiligd mogen zijn, een kruisraket van onze 'vriend uit het oosten' legt geheid een compleet centrum plat. Als hij er drie afvuurt is het volledig gedaan met onze ict. Dit fenomeen is al jaren geleden aangekaart en er zijn toen gedecentraliseerde systemen ontworpen met een maasvormig netwerk van kleine mini-datacenters, die via glasvezels met elkaar verbonden zijn. Door de toenmalige bezuinigingen op defensie is er nooit een praktische implementatie gekomen. De techniek is inmiddels voortgeschreden, de dreiging van zo'n scenario is zeker niet minder geworden en er is meer geld beschikbaar.

Diverse start-ups en al wat meer gerenommeerde bedrijven (bv Nutanix, Simplivity, Zerto, Rubrik, Netapp, Vmware, etc.) leveren software en hardware waarmee je gemakkelijk een datacenter cloud kan maken met 64, 128 of zelfs wel 256 nodes, die allemaal op een andere locatie kunnen staan en die de applicaties dynamisch kunnen verdelen over meerdere nodes die naadloos elkaars backup kunnen zijn. Daarnaast zijn de distributie en loadbalancings mechanismen met behulp van AI (artificial intelligence) tot grote hoogten gestegen.

Door geavanceerde snapshot technieken kunnen ook mogelijke cyberaanvallen gemakkelijk gerepareerd worden. Ook de uitgezonden operationele onderdelen als deployed eenheden en schepen kunnen gemakkelijk in zo'n datacenter grid worden opgenomen of ter plekke een mini grid vormen. Onze vriend uit het oosten moet bij toepassing van dergelijke volledig gedecentraliseerde omgevingen niet drie maar honderden kruisraketten afvuren om het systeem en alle applicaties volledig uit te schakelen. Omdat de datacenter functionaliteit hiermee volledig verspreid wordt over het land, van noord tot zuid en van oost tot west, is een bijkomend voordeel dat de kans op uitval door stroomstoringen ook veel kleiner is geworden. Met het NAFIN glasvezelnetwerk en zijn gemoderniseerde infrastructuur heeft defensie een prachtige basis om dit te realiseren.

Operating system resilience

Een derde resilience onderwerp dat ik wil behandelen is het operating system. Bekend zijn de diverse cyber attacks, die zelfs complete containerterminals kunnen platleggen. De schade voor MAERSK bedroeg volgens een spreker op het laatste NIDV cyber congres honderden miljoenen euro's. Bij nadere analyse blijkt dat in de meeste gevallen dergelijke aanvallen altijd plaatsvinden op bepaalde specifieke Windows software en releases.

Hier kunnen we de les toepassen van de efficiëntie in de aardappelteelt in de Andes, jaren geleden gestuurd door de UN. Uit efficiëntie overwegingen moesten de Andesboeren een soort aardappel gaan telen die veel meer opbrengst had dan de vele soorten aardappelrassen (4000) die daarvoor geteeld werden. Toen er na jaren goede opbrengst een keer een virus onder dit aardappelras uitbrak was er hongersnood in de Andes. In vroeger tijden brak het virus uit in enkele rassen, maar de andere rassen hadden daar geen last van. Toen men nog maar een ras had was er gelijk een hongersnood toen dat ras getroffen werd.

Als we de parallel trekken naar de ict en operating systems, is bewezen dat heel vaak een virus uitbraak slechts een specifiek platform treft en niet alle platformen. Daarom is het voor een organisatie waar resilience zeer belangrijk is niet ´alle eieren in een mandje´ te leggen en ervoor te zorgen dat er meerdere smaken zijn die gebruikt kunnen worden. In de ict-praktijk van vandaag betekent dit dat je bijvoorbeeld Windows naast Chromeos of een Linux smaak moet gebruiken en op mobiel gebied niet alleen IOS maar ook Android. Door het spreiden over verschillende platformen en software geschikt te maken op al deze platformen te draaien maak je de organisatie zeer weerbaar tegen allerlei aanvallen. En als het dan al zou gebeuren kan je cruciale bedrijfsfuncties uitvoeren op het niet getroffen platform.

Het kost extra moeite en beheerinspanningen om meerdere platformen te ondersteunen, maar de extra kosten wegen naar mijn inschatting ruim op tegen het risico volledig uitgeschakeld te worden. Daarnaast wordt de leveranciersafhankelijkheid sterk verminderd hetgeen ook een niet onbelangrijk resilience aspect is met ook sterke financiële voordelen.

Conclusie: resilience operationele noodzaak

Het onderwerp resilience is zeker voor defensie heel belangrijk en cruciaal voor ongestoorde operaties. In het voorgaande heb ik slechts drie aspecten behandeld, maar er is veel meer dat aandacht verdiend. Duidelijk is dat vanwege het uitgangspunt 'als alles stilvalt defensie doorgaat', defensie afwijkende technieken en concepten moet hanteren dan de ict die bedrijven toepassen. Dus niet alles uit de cloud in een gehuurd datacenter, niet gebruik maken van één mobiele operator, niet alles concentreren op enkele plaatsen, geen gebruik maken van één gestandaardiseerd operating system en werkplek, kortom defensie dient tegendraadse oplossingen te kiezen net zoals de boeren in de Andes die meerdere aardappelrassen moeten telen om te overleven in rampscenario's.

Deze filosofie gaat in tegen het wijdverbreide efficiëntiestreven van 'gewone' bedrijven maar is een keiharde operationele noodzaak voor defensie.