Cyber is overduidelijk een voorvoegsel welke in meer en mindere mate binnen een Hype geplaatst kan worden. Het verschijnsel Cyber wordt duidelijk met alle achtervoegsels een uiting met zogenoemde 'Power House' effecten. Dat wil zeggen dat het woord een gevolg van een zichzelf versterkend mechanisme is. Het Hypen van Cyber is binnen de digitale revolutie dan ook een fenomeen op zich geworden. Nu is Cyber met alle achtervoegsels een zelfstandig naamwoord, maar ook wordt Cyber als werkwoord gekunsteld en zijn er Cyberians. Dit is de groep die Hyper Connected is binnen de 'Cognoscenti', ons kent ons, en van, en door dezelfde mystieke gemeenschap elkaar verbinden en verbonden worden.

Binnen het domein Business Continuity Management omvat Cyber en de daarmee verband houdende digitale technologie binnen het werkingsveld van organisaties. Specifiek hanteert BCM Academy de normatieve ontwikkelprincipes en entiteiten van 'Cyber' als de digitale communicatie en informatie technologie, het bereik, inzet en gebruik ervan gericht op Virtuele en Reële (concrete en abstracte) toepasbaarheid en werking. Binnen dit bereik is Cyber Security niet enkel een 'hot topic', maar ook een wakkerligger en grenst zonder control aan een welhaast mystieke perceptie. Wij benoemen dan ook liever de Digitale Veiligheid in plaats van Cyber Security.

Het gehele Cyber domein omvat een welhaast gordiaanse knoop, onontwarbaar en volgens de mythe samen met de 'strijdwagen' tot het middelpunt van de wereld behorend. Op een veelheid van aspecten zal de analogie aansluiten. Binnen het werkingsveld van Business Continuity Management is het een gemanaged en een uiterst kritisch procesgebied die door juist de uiteinden van de 'hypothetische' knoop te ontdekken of in beeld te hebben en te houden het 'werkingsveld' te exploreren en te ontwarren.

Cyber Security, Digitale Veiligheid wordt binnen de dagelijkse praktijk vaak nogal oneigenlijk van labels voorzien die voortkomen uit het willen 'meeliften' op de hype, de onzekerheid en soms aan de angst van het oncomfortabele en kwetsbare weerstand te bieden . Expertviews tonen aan dat product, en dienstenaanbieders nogal eens volgaarne gebruik maken van de Cyber Hype echter dan als een façade, dan wel met waaninzet bijdragen aan 'schijnzekerheden'. Misvattingen rondom invulling van het stelsel van maatregelen zijn binnen het gehele spectrum aanwezig. Dit van het ontwikkelen van beleid tot effectief risico management en opvolgende analyse van de business impact tot het testen, auditen en maintenance van het stelsel van maatregelen. Simpelweg is er een toenemende mismatch tussen geadapteerd en ontwikkeld beleid en de tactisch operationele invulling ervan. Expert, ervarings en actuele onderzoeks analyse van BCM Academy (TIC³, Trends In Cybersecurity 2017 | 2020) presenteert een toenemende afstand tussen het vereiste optimum en de actuele 'stand van zaken', op de geïndexeerde schaal van het Business Continuity Management 'volwassenheidsmodel'.

Opmerkelijk negatief verassend is dat de businessplannen van organisaties weliswaar ICT, Cyber(security) digitale veiligheid op de 'bucketlist' hebben staan, maar de 'buitenkant' beduidend krachtiger ontwikkelen dan de binnenkant van de 'business'. 'Mooi van buiten, rot van binnen is in veel opzichten de dag praktijk binnen de business as usual. Practise what you preach en teach as you preach is zonder twijfel een zacht dwingende en dringende aanrader. Slaap zacht en 'stay in the dark' is voor velen dan ook een aanbeveling omdat simpelweg de ontstane kloof tussen de vereiste noodzakelijke ambitie en de stand van zaken zonder 'aan~ingrijpen' onoverbrugbaar is. Minding the Gap en Bridging the Gap is een door BCM Academy ontwikkelde methode die in elk geval de future view binnen bereik plaatst en ondertussen de organisatie door en over barrières brengt en tegelijkertijd afrekent met ballast veroorzakende en remmende 'traditionals'.

Binnen "Cyber', de Digitale Veiligheid is inderdaad de analogie met Troje een uiterst gepaste en bovendien een wetenschappelijk toepasbare. Evenals de gordiaanse knoop is ook Troje onderdeel van een strijdtoneel, economische

> *"Evenals de gordiaanse knoop is ook Troje onderdeel van een strijdtoneel, economische belangen en omringt door mythologie en*

belangen en omringt door mythologie en technologie Achilles en Hektor nemen wij in hetzelfde rijtje mee. Om binnen een Risico Analyse Model (RAM) een reëel direct toepasbaar resultaat te presenteren Is de Slice Of Life (SOL) theorie een uitermate effectieve.

SOL gaat uit van een 'open einde' overeenkomstig de Tech & Cyberpush en anderzijds de realistische weergave binnen de organisatie dialoog van de actuele proceswerking en de ontwikkeling van conflict en risico opbouw/vorming. Dus enerzijds de hyperrealistische weergave (Slice), anderzijds de techniekontwikkeling van conflictexpositie (Life). SOL is een krachtig instrument zonder direct in Cyber en Tech details en basale ineffectieve 'oplossingen' verloren te gaan. Volgens Cruyff; "Als wij de bal hebben, kunnen hun niet scoren" is in elk geval een waarheid daarbinnen. Cyber Strijdtonelen van nu vereisen hyper doordachte en ultra snelle actie. Inderdaad, met een open einde.