De voor organisaties, de sectoren zelf niet op te lossen problemen, de crises waarin zij zich bevinden kan bij een aanslag op primaire processen tot controversieel ingrijpen leiden door regelgevers, of zelfs op mondiaal niveau tot uitsluitingen en afsluitingen. De dan op te lossen crises is één van de lastigste, treft iedereen hard en heeft blijvende negatieve effecten.

Survival of the most adaptable

De financiële 'Meltdown' van 2009 heeft ook nu nog (blijvend) negatief vetrouwenseffect. Het vertrouwen is slechts deels hersteld na een reeks van grootschalige, controversiële harmoniserende injecties van 'openbaar geld' in het bankwezensysteem. Substantiële versterkingen van een mondiaal governance-kader, waaronder organisaties zoals de Raad voor financiële stabiliteit, de Bank voor internationale betrekkingen en het Internationaal Monetair Fonds. Nu nog maakt de onbalans deel uit van zowel het financiële bankensysteem, maar ook van landeigen economieën.

In een Cyber crisis, er is geen duidelijk equivalent zoals dat van Greenspan, destijds, geplaatst. Wellicht nog belangrijker, een mondiaal bestuurskader is gewoonweg nu niet te bouwen, omdat een cyberspace crisis zich kan ontwikkelen als gevolg van unilaterale acties van juist een natie, of staat. Een valuta-of handelsoorlog zou een beter vergelijk zijn met een 'cyber voorbeeld' immers, als landen het niet eens zijn over grondregels, de doelstellingen en geen rekenschap gehouden wordt met, notie ontbreekt van technische mondiale afspraken en akkoorden, verliest immers alles zijn doel en waarde. Indien dit fenomeen dus politiek, diplomatiek, en/of defensiegericht richting gaat krijgen kunnen 'organisatiematige' normen enkel voor crisisacceptatie kiezen 'Survival of the most adaptable' is dan nog het enige wat telt.

Een select aan tal wetenschappers betogen dat een juist niet-gouvernementele Cyber norm ingezet door experts en bestuurders, zoals de wereldwijde Commissie voor de stabiliteit in cyberspace, een belangrijke rol kunnen spelen bij het helpen om dit probleem van juiste waarden en inzet te voorzien. Oplossingen kunnen ook worden ontwikkeld in groepen gelijkgestemde landen, zoals de EU, en vervolgens uitbreiden tot bredere, mondiale werking. Ook hier, treffend vergelijk met het financiële systeem en de maatregelstelsels. Dus maatregelgericht in plaatst van theoretische 'convenanten' en 'afspraken'. Ministeries van Financiën en gouverneurs van centrale banken zijn zich wellicht het meeste bewust wat 'systemische onrust' echt betekent. Zij zijn, alhoewel relatief éénzijdig begonnen met het werken aan voorstellen voor grensoverschrijdende Cyber crisissimulatie oefeningen en ontwikkelen CrisisTrails juist vanuit beheersstelsels.

Kennishiaten en illusionisme

Binnen het domein Business Continuity Management, en specifiek gericht op de vitale 'ICT keten' en het primaire proces van organisaties zijn er toenemend significante kennishiaten welke enkel groter (dreigen te) worden. Dit blijkt niet enkel uit expert views, resultaten van Audits, maar ook uit stresstesten en analyse van reeds manifest geworden calamiteiten en disrupties. Voorzichtig kan worden aangenomen dat sommige noodzakelijke 'inhaalslagen' nu al niet meer gemaakt kunnen worden. En ronduit verontrustend is de constatering dat organisaties met kritische ketenafhankelijkheden juist ook blootstaan aan 'zwakke partners' maakt het kwetsbaarheidsoppervlak enkel groter.

Wellicht wat kort door de bocht, blijken de ICT (beheers)organisaties niet geëquipeerd om juist (en effectief) om te gaan met 'nieuw'. Aan de achter, en de voorkant wordt weliswaar met 'schijnveilige' applicaties en slimmigheden het een en ander afgedekt, maar procesmatig, infrastructureel stapelen de kwetsbaarheden en afhankelijkheden op. Immers het procesmatige en ICT (NIS),

> *"'Survival of the most adaptable' is dan het enige wat telt"*

netwerken en informatiesystemen en NOS, (Netwerk Operating Systemen) kwetsbaarheidsoppervlak neemt exponentieel toe en de 'oude kennis' (be)reikt niet de behoefte welke nu essentieel is. Old scool denken en doen is nu de grootste 'beperkter'.

'Platte technologie' kennis is relatief snel en adequaat te mobiliseren, maar significante kennis hiaten over de plaats en de inter-connecties van de zwakke knopen in de veiligheidsketen is (nog) ver te zoeken en sterk, zelfs toenemend ernstig onderontwikkeld. "Betrouwbare, onpartijdige, uitgebreide en algemeen toegankelijke" gegevens over de frequentie en de economische impact van onder andere cyberaanvallen zijn nog steeds zeldzaam. Recente inspanningen bieden dan voor enkele organisaties in de 'problemen' een overleving, maar sectorgenoten (welke niet getroffen zijn) blijven de illusie van onschendbaarheid sterk aanhangen. Analyse, afgestemde (theoretische) kaders en informatie is van vitaal belang om te helpen begrijpen welke gebieden van de 'economie' dringende interventie nodig hebben, zij het in termen van bewustmakingscampagnes, toegewijde prikkels, of regelgeving.

Bestuurders beseffen slechts in mate dat noodzaak, maar ook de urgentie aanwezig is juist nu de 'harde noten' te kraken en juist zelf de disruptie in te zetten om beter geëquipeerd te zijn voor de volgende rondes welke enkel nog complexer en kritischer worden. De werkelijkheid van de hiaten en de illusie van onschendbaarheid dienen een 'make-over' te krijgen. Stabiliteit en continuïteit eist daarom ook gezonde (zelf)reflectie.